

» Kontron User's Guide «

smartCore Express SMA200 BIOS

BIOS, Driver & Software Information
Document Revision 102

» Table of Contents «

1	User Information	4
1.1	About this Document	4
1.2	Copyright Notice	4
1.3	Trademarks	4
1.4	Standards	4
1.5	Warranty	4
1.6	Technical Support	5
1.7	Environmental Protection Statement	5
1.8	RoHS Commitment	5
1.8.1	RoHS Compatible Product Design	6
1.8.2	RoHS Compliant Production Process	6
1.8.3	WEEE Application	6
1.9	Swiss Quality	6
1.10	The Swiss Association for Quality and Management Systems	7
2	Introduction	8
2.1	Standard Features	8
2.2	Incompatibilities	8
3	Operating Systems Compatibility	9
3.1	Microsoft Windows	9
3.2	Microsoft Windows XPe	9
3.3	Microsoft Windows CE	9
3.3.1	CE4.2 / CE5.0	9
3.3.2	CE6.0	9
3.4	Linux	10
3.4.1	SLAX	10
3.4.2	ELinOS	10
3.4.3	What is ELinOS?	10
3.5	Real-time OS	10
3.5.1	QNX	10
3.5.2	VxWorks	10

4	Driver Installation	11
4.1	Windows 2000 & XP	11
4.1.1	Chipset	12
4.1.2	VGA.....	12
4.1.3	LAN.....	13
4.1.4	AC97-Sound.....	14
4.1.5	RAID	14
4.2	Display Driver and Control Panel.....	17
4.3	AC97 Sound Driver and Control Panel.....	19
4.4	SpeedStep	20
4.5	SpeedStep Performance Control	20
4.5.1	Set up Power Management	21
5	The Special Function Interface (SFI)	22
5.1	INT15h SFR Functions.....	22
5.2	Int15 Emulator Driver for Windows	24
5.2.1	Int15 Hardware	24
5.2.2	Int15 Windows Software	25
5.2.3	Driver Installation W2k/XP	25
5.2.4	Driver Installation Windows-NT	26
5.2.5	Programming Int15dl Interface under Windows	26
6	Software.....	28
6.1	Windows Int15 Tool	28
6.2	Int15 Windows Software	28
7	Diagnostics	29
7.1	Phoenix SecureCore™ Checkpoint Lists for the SMA200	29
7.1.1	POST Code Checkpoints.....	29
8	BIOS	32
8.1	BIOS History	32
8.2	Specifications of the BIOS	33
8.3	Core BIOS Functions	34
8.4	Core BIOS Download	36
8.5	BIOS Setup	37
8.5.1	Main Menu.....	37

8.5.2	Advanced	38
8.5.3	Advanced I/O Configuration	38
8.5.4	Advanced Console Redirection	39
8.5.5	Intel	39
8.5.6	Intel CPU Control	40
8.5.7	Intel CPU Thermal Control	40
8.5.8	Intel Poulsbo Control	41
8.5.9	Intel Poulsbo PCI Express Control	41
8.5.10	Intel Poulsbo USB Control	42
8.5.11	Intel Video Control	42
8.5.12	Security	43
8.5.13	Boot	43
8.5.14	Exit	44
8.6	CMOS RAM Map	45
9	Appendix A: Document Revision History	50
10	Index	51

1 User Information

1.1 About this Document

This document provides information about products from Kontron AG and/or its subsidiaries. No warranty of suitability, purpose, or fitness is implied. While every attempt has been made to ensure that the information in this document is accurate, the information contained within is supplied "as-is" and is subject to change without notice.

For the circuits, descriptions and tables indicated, Kontron assumes no responsibility as far as patents or other rights of third parties are concerned.

1.2 Copyright Notice

Copyright[®] 2003-2010 Kontron AG

All rights reserved. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron AG.

1.3 Trademarks

MICROSPACE[®], smartModule[®], smartCore[®]Express and DIGITAL-LOGIC[®] are trademarks or registered trademarks of Kontron Compact Computers AG. Kontron is a trademark or registered trademark of Kontron AG.

The following lists some of the trademarks of components used in this product.

- » IBM, XT, AT, PS/2 and Personal System/2 are trademarks of International Business Machines Corp.
- » Microsoft is a registered trademark of Microsoft Corp.
- » Intel is a registered trademark of Intel Corp.

All other products and trademarks mentioned in this manual are trademarks of their respective owners.

1.4 Standards

Kontron AG is certified to ISO 9000 standards.

1.5 Warranty

This Kontron AG product is warranted against defects in material and workmanship for the warranty period from the date of shipment. During the warranty period, Kontron AG will, at its discretion, decide to repair or replace defective products.

Within the warranty period, the repair of products is free of charge as long as warranty conditions are observed.

The warranty does not apply to defects resulting from improper or inadequate maintenance or handling by the buyer, unauthorized modification or misuse, operation outside of the product's environmental specifications or improper installation or maintenance.

Kontron AG will not be responsible for any defects or damages to other products not supplied by Kontron AG that are caused by a faulty Kontron AG product.

1.6 Technical Support

Technicians and engineers from Kontron AG and/or its subsidiaries are available for technical support. We are committed to making our products easy to use and will help you use our products in your systems.

Please consult our website at <http://www.kcc-ag.ch/index.php?id=products-download> for the latest product documentation, BIOS, drivers, tools and software information.

For technical support consult <http://support.kcc-ag.ch/>.

1.7 Environmental Protection Statement

This product has been manufactured to satisfy environmental protection requirements wherever possible. Many of the components used (structural parts, printed circuit boards, connectors, batteries, etc.) are capable of being recycled. Final disposal of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations. All components within this product fulfill the requirements of the RoHS (Restriction of Hazardous Substances Directive). The product is soldered with a lead free process.

1.8 RoHS Commitment

Kontron Compact Computers AG (Switzerland) is committed to develop and produce environmentally friendly products according to the Restriction of Hazardous Substances (RoHS) Directive (2002/95/EC) and the Waste Electrical and Electronic Equipment (WEEE) Directive (2002/96/EC) established by the European Union. The RoHS directive was adopted in February 2003 by the European Union and came into effect on July 1, 2006. It is not a law but a directive, which restricts the use of six hazardous materials in the manufacturing of various types of electronic and electrical equipment. It is closely linked with the Waste Electrical and Electronic Equipment Directive (WEEE) 2002/96/EC, which has set targets for collection, recycling and recovery of electrical goods and is part of a legislative initiative to solve the problem of huge amounts of toxic e-waste.

Each European Union member state is adopting its own enforcement and implementation policies using the directive as a guide. Therefore, there could be as many different versions of the law as there are states in the EU. Additionally, non-EU countries like China, Japan, or states in the U.S. such as California may have their own regulations for green products, which are similar, but not identical, to the RoHS directive.

RoHS is often referred to as the "lead-free" directive but it restricts the use of the following substances:

- » Lead
- » Mercury
- » Cadmium
- » Chromium VI
- » PBB and PBDE

The maximum allowable concentration of any of the above mentioned substances is 0.1% (except for Cadmium, which is limited to 0.01%) by weight of homogeneous material. This means that the limits do not apply to the weight of the finished product, or even to a component but to any single substance that could (theoretically) be separated mechanically.

1.8.1 RoHS Compatible Product Design

All standard products from Kontron Compact Computers (KCC) comply with RoHS legislation.

Since July 1, 2006, there has been a strict adherence to the use of RoHS compliant electronic and mechanical components during the design-in phase of all KCC standard products.

1.8.2 RoHS Compliant Production Process

KCC selects external suppliers that are capable of producing RoHS compliant devices verified by:

- » A confirmation from the supplier indicating that their production processes and resulting devices are RoHS compliant.
- » If there is any doubt of the RoHS compliancy, the concentration of the previously mentioned substances in a produced device will be measured. These measurements are carried out by an accredited laboratory.

1.8.3 WEEE Application

The WEEE directive is closely related to the RoHS directive and applies to the following devices:

- » Large and small household appliances
- » IT equipment
- » Telecommunications equipment (although infrastructure equipment is exempt in some countries)
- » Consumer equipment
- » Lighting equipment – including light bulbs
- » Electronic and electrical tools
- » Toys, leisure and sports equipment
- » Automatic dispensers

It does not apply to fixed industrial plants and tools. The compliance is the responsibility of the company that brings the product to market, as defined in the directive. Components and sub-assemblies are not subject to product compliance. In other words, since Kontron Compact Computers AG does not deliver ready-made products to end users the WEEE directive is not applicable for KCC. Users are nevertheless encouraged to properly recycle all electronic products that have reached the end of their life cycle.

1.9 Swiss Quality

- » 100% Made in Switzerland
- » This product was not manufactured by employees earning piecework wages
- » This product was manufactured in humane work conditions
- » All employees who worked on this product are paid customary Swiss market wages and are insured
- » ISO 9000:2001 (quality management system)

1.10 The Swiss Association for Quality and Management Systems

The Swiss Association for Quality and Management Systems (SQS) provides certification and assessment services for all types of industries and services. SQS certificates are accepted worldwide thanks to accreditation by the Swiss Accreditation Service (SAS), active membership in the International Certification Network, IQNet, and co-operation contracts/agreements with accredited partners.

www.sqs.ch

The SQS Certificate ISO 9001:2000 has been issued to Kontron Compact Computers AG in the field of development, manufacturing and sales of embedded computer boards, embedded computer modules and computer systems. The certification is valid for three years at which time an audit is performed for recertification.

2 Introduction

The smartCore Express SMA200 BIOS is used on Kontron Compact Computers' (KCC) 200 series of products.

2.1 Standard Features

- » Phoenix SecureCore BIOS ROM

2.2 Incompatibilities

t.b.d.**

3 Operating Systems Compatibility

3.1 Microsoft Windows

Kontron Compact Computers (KCC) recommends the following Windows operating systems in combination with the chipset listed below:

- » Intel A200: Windows Vista, Windows XP (SP2)

It is not recommended to install an older Windows OS, such as Windows 95/98/ME/NT4/2K, because of incomplete driver support from the chip manufacturer.

3.2 Microsoft Windows XPe

KCC provides a Windows XPe (SP2) Board Support Package for the following chipset:

Intel A200:

<http://www.kcc-ag.ch/index.php?id=294&dir=BSP/INTEL A200&mountpoint=46>

A CompactFlash with a copy of "Evaluation Windows XPe" pre-installed can be ordered for testing purposes:

- » Intel A200 Article number 816060

3.3 Microsoft Windows CE

3.3.1 CE4.2 / CE5.0

KCC works in cooperation with Pfaadtsoft and therefore recommends using the WINCE 4.2/5.0 Board Support Package (BSP) developed especially for this product.

There are also DEMO Windows CE 4.2 / 5.0 images available for free at:

<http://dlag.pfaadtsoft.de/>

3.3.2 CE6.0

Kontron Compact Computers provides a Windows CE 6.0 BSP for the following chipset:

Intel A200:

<http://www.kcc-ag.ch/index.php?id=294&filename=CE6.zip&dir=BSP/A200&task=download&mountpoint=46>

You can order a CompactFlash with a pre-installed copy of "Evaluation Windows CE6" for testing purposes.

- » Intel A200 Article number 816070

3.4 Linux

3.4.1 SLAX

Kontron Compact Computers (KCC) provides a Linux distribution (Kernel 2.6.24) for the following chipsets:

AMD LX800, Intel 855, Intel 945, Intel A200

Follow this link to download the BSP / Demo SLAX Linux:

<http://www.kcc-ag.ch/index.php?id=294&dir=BSP/SLAX-BSP&mountpoint=46>

A CompactFlash with a pre-installed copy of Linux for testing purposes can be ordered:

» Linux Article Number 816030

The distribution is based on the SLAX Linux. For more information, updates and plug-ins, visit: www.slax.org

3.4.2 ELinOS

KCC works in cooperation with SYSGO and therefore recommends using the ELinOS Linux distribution.

<http://www.elinos.com/>

SYSGO has developed a board support package (BSP) for the Pentium M and the Pentium BX/TX chipset-based products for ELinOS. If you are interested or if you have any questions about ELinOS, please contact SYSGO directly.

3.4.3 What is ELinOS?

ELinOS is a development environment based on Linux for the creation of embedded systems for intelligent devices. With ELinOS the memory demand of Linux is reduced to less than 1MB ROM and 2MB RAM. In this manner Linux can, for the first time, conform to the reduced hardware conditions of embedded systems. Even in this basic configuration, Linux offers largely the same functionality which made it so popular in the server and desktop field. By virtue of access to the constantly growing number of Linux components, the basic system can be expanded at any time.

The core of ELinOS is a Linux distribution custom-tailored to the embedded systems currently sold. Besides the well-known Linux version for x86, ELinOS also supports PowerPC-, ARM-, MIPS-, and SH3-platforms which are very popular in the embedded field.

The emphasis of the current version of ELinOS is on the new CoTools, CODEO and COGNITO. CODEO is Eclipse based and provides additional plug-ins for project management and target communication, which substantially improves the ease of development of applications with ELinOS. COGNITO is a further integrated tool for the analysis of system performance. It permits the collection, recording and display of all system information and facilitates the fast optimization of software for intelligent devices.

ELinOS has been updated to the new version of the GNU tool chain and contains the stable Linux Kernel starting with version 2.4.25; it has integration of Java and the real-time extensions RTAI 3.0 for hard real-time requirements. The package is complemented with Carrier Grade Extensions such as IPv6, IPSec, SNMP, etc., for the use of Linux in applications in the telecommunications market.

3.5 Real-time OS

3.5.1 QNX

Download a demo image from the following website: <https://www.qnx.com/account/Login.html?logout=1>

3.5.2 VxWorks

Please contact Wind River for VxWorks support: www.windriver.com

4 Driver Installation

4.1 Windows 2000 & XP

On the Product CD you will find all the tools and drivers you'll need to work with the product. If you are unsure how current your software is, please visit our website to get the latest releases!

<http://www.kcc-ag.ch/index.php?id=products-download>

A correct installation of Windows is required for the following steps.

1. Close all applications before beginning with the driver installation!
2. Put the Kontron Compact Computers Product CD into the CD-drive. The start menu should appear automatically.
3. Select: Drivers/WinXP.
If there is no menu then manually open up the CD on the desktop.

Board-Support-Package for Intel Atom200 Based Products - V2.00



[HOME](#) [MANUALS](#) [BIOS](#) [BSP](#) [DRIVERS](#) [TOOLS](#) [EXIT](#)

This CD contains all manuals,drivers,BSP,tools and bios for the following products:
MPC25-26, MSB200, MSM200S, MSM200X/XU/XP, SMA200, SMA200DK1

Legal Notice:

Kontron Compact Computers AG, smartModule, smartCore, MICROSPACE and MicroDesign are registered trademarks and are property of Kontron Compact Computers AG, Switzerland.
All other brandnames, trademarks and registered trademarks are property of their respective owners.

All data is for information purposes only, is subject to change, and is not guaranteed for legal purposes.
Information in this document has been carefully checked and is believed to be accurate, however, no responsibility is assumed for inaccuracies.

© Copyright 2010
Kontron Compact Computers AG, Switzerland
All rights reserved.



Kontron
Compact Computers AG
Nordstrasse 11/F
CH-4542 Luterbach
Switzerland

Tel. +41 32 681 58 00
Fax +41 32 681 58 01

saleskcc@kontron.com
supportkcc@kontron.com

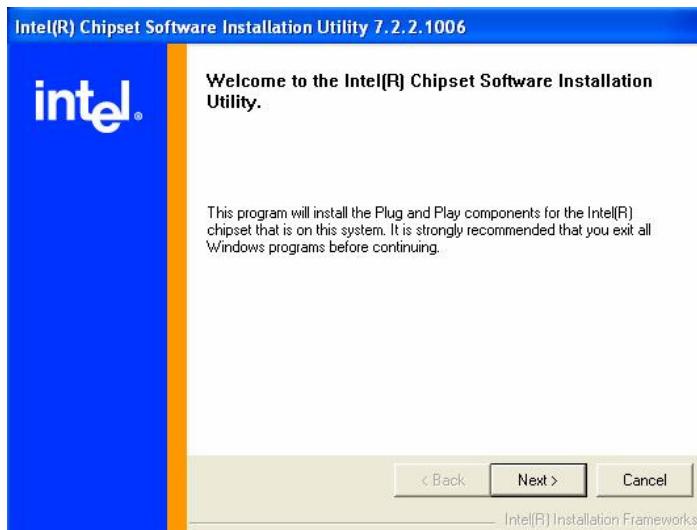
<http://www.kcc-ag.ch>

SupportCenter Manual

4.1.1 Chipset

Driver: x:\drivers\SMA200\chipset\

Double click on setup.exe and follow the instructions:

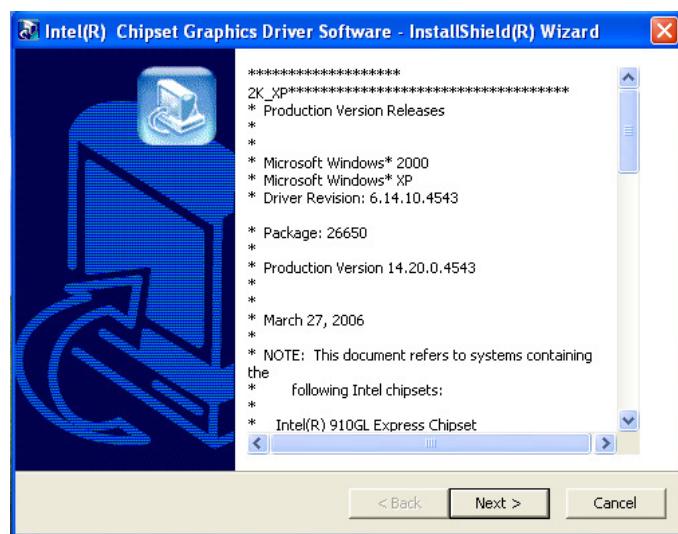


Reboot the system after installation.

4.1.2 VGA

Driver: x:\drivers\SMA200\VGA

Double click on setup.exe; follow the instructions:



Reboot the system after the installation.

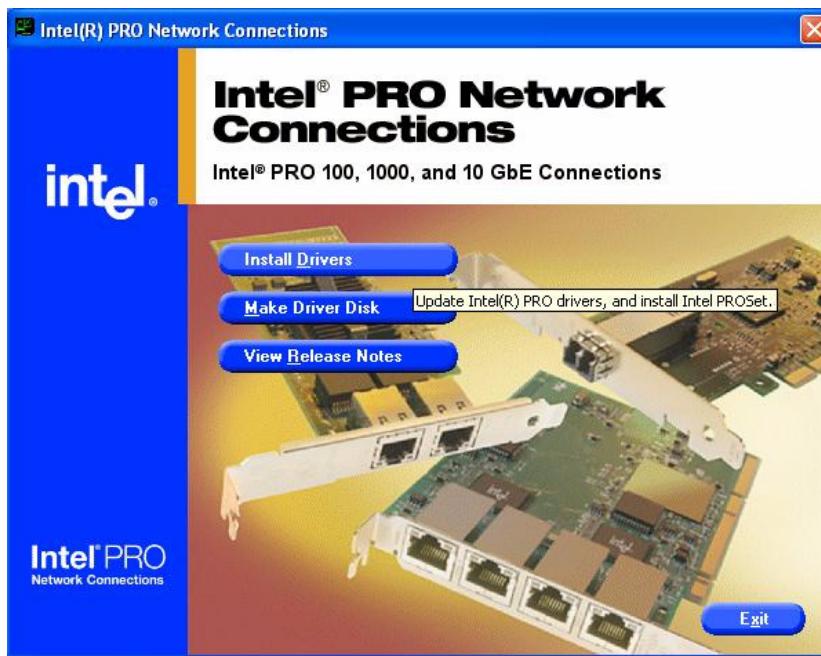
4.1.3 LAN

Driver: x:\drivers\SMA200\Ethernet

Double click on setup.exe and follow the instructions:



Or double click on autorun.exe and follow the instructions:



Click "Install Drivers".

4.1.4 AC97-Sound

Driver: x:\drivers\SMA200\Audio

Double click on setup.exe and follow the instructions:



4.1.5 RAID

Raid is not supported on the SMA200

Loading the driver during OS installation

Overview

The Silicon Image SATA driver must be loaded during the operating system installation using the **F6** installation method in order to install an operating system onto a hard drive.

F6 installation method

The **F6** installation method requires a floppy with the driver files.

F6 floppy driver:

Driver: x:\drivers\SMA200\SATA\3132_x86_1.0.22.0_logo.zip

F6 Installation Steps

To install the Intel® Matrix Storage Manager driver using the **F6** installation method, complete the following steps:

1. Press the **<F6>** key at the beginning of the Windows XP setup (during the text-mode phase) when prompted in the status line with the "Press F6 if you need to install a third party SCSI or RAID driver" message.



Note After pressing **F6**, nothing will happen immediately; setup will temporarily continue loading drivers and then you will be prompted with a screen to load support for mass storage device(s).

2. Press the **<Z>** key to specify an additional device.



3. Insert the floppy disk containing the driver files when you see the following prompt: "Please insert the disk labeled Manufacturer-supplied hardware support disk into Drive A:" and press the <Enter> key. Refer to Automatic **F6** Floppy Creation for instructions.
4. Select the "Silicon Image SiI 3132 SATALink Controller for Windows XP/Server2003" entry and press the <Enter> key.



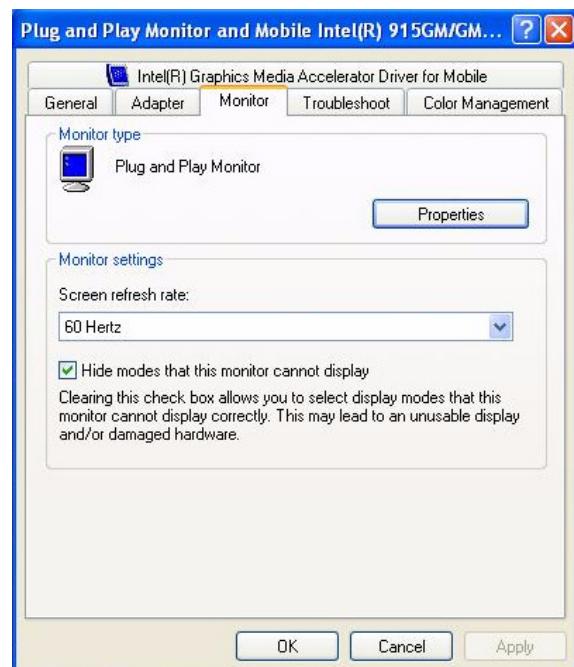
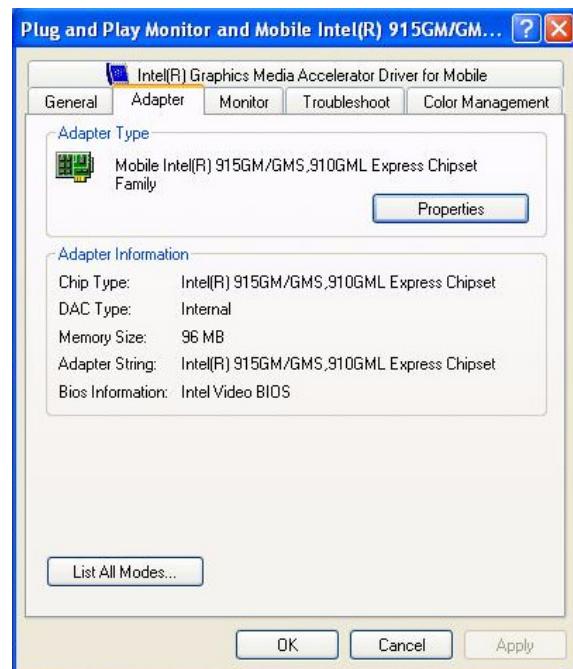
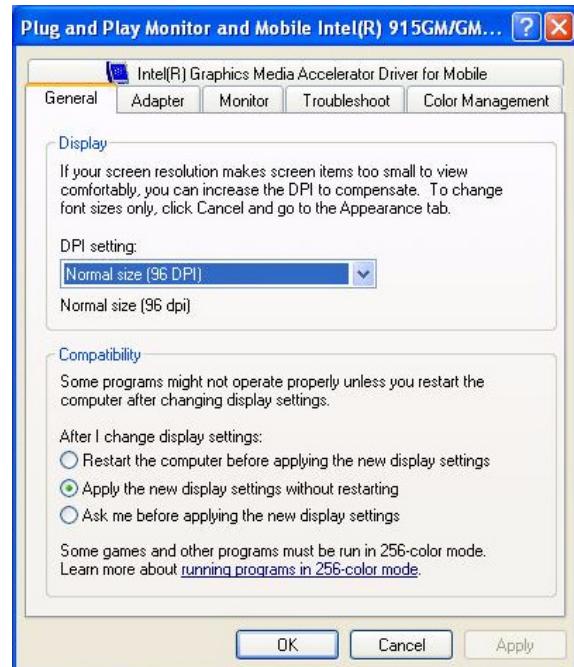
5. Press the <Enter> key to confirm.

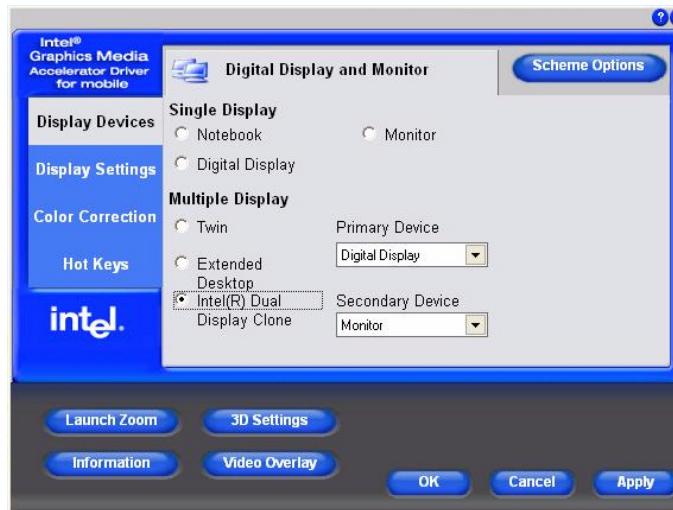
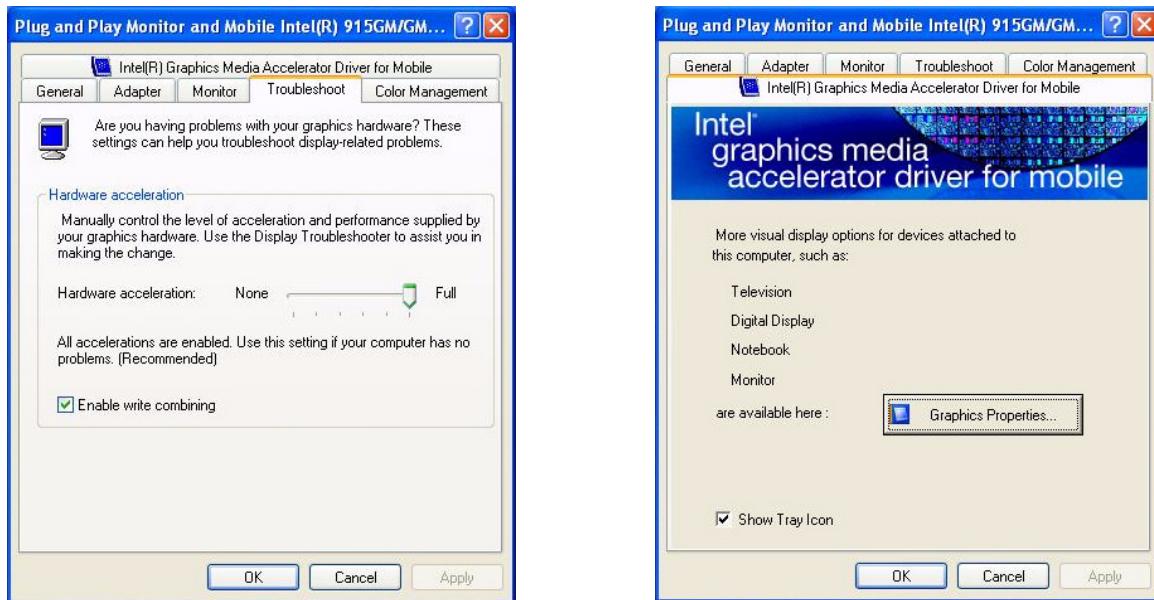
At this point, you have successfully **F6** installed the Silicon Image SATA driver and Windows XP setup should continue. Leave the floppy disk in the floppy drive until the system reboots itself because the Windows setup will need to copy the files again from the floppy to the Windows installation folders. After Windows setup has copied these files again, remove the floppy diskette so that Windows setup can reboot as needed.

4.2 Display Driver and Control Panel

Start / Control Panel / Appearance and Themes / Display Properties / Settings tab

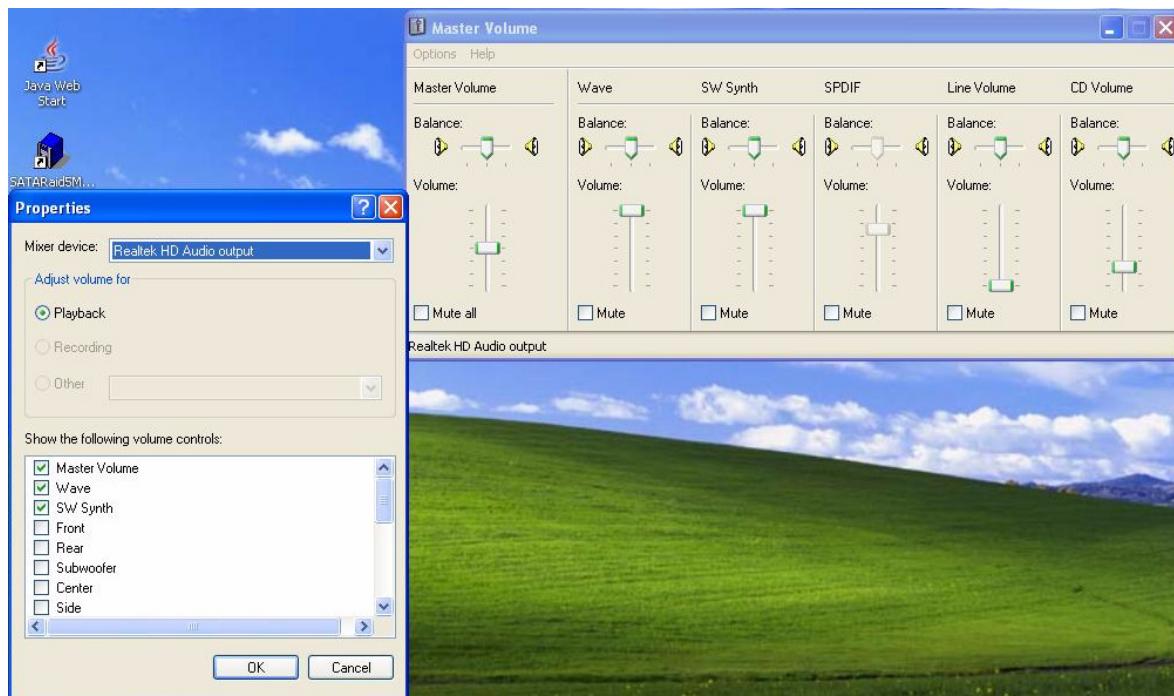
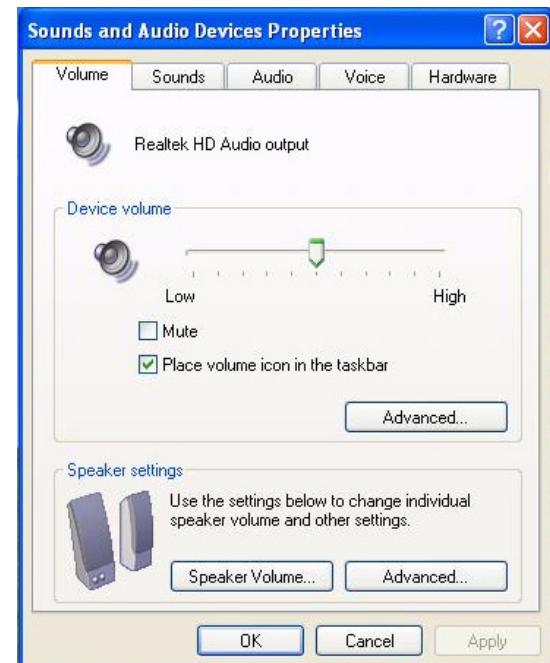
Enter the following settings:



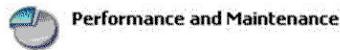


4.3 AC97 Sound Driver and Control Panel

Sound Settings:



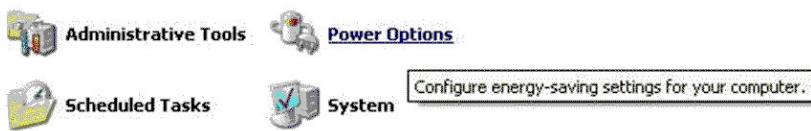
4.4 SpeedStep



Pick a task...

- See basic information about your computer
- Adjust visual effects
- Free up space on your hard disk
- Back up your data
- Rearrange items on your hard disk to make programs run faster

or pick a Control Panel icon



4.5 SpeedStep Performance Control

The Pentium-M improved the SpeedStep mechanism by adding a third power scheme in addition to the low-power and the full-performance modes. This new mode is called adaptive mode, and allows the frequency and voltage to switch according to the CPU activity. The CPU uses a low-power mode by default, but when its activity increases, it switches itself very quickly into full-performance mode. This new power scheme is very pleasant to use, because it allows full CPU speed only when needed. Of course, power consumption depends on the CPU activity, and the more the CPU is used, the more it consumes power.

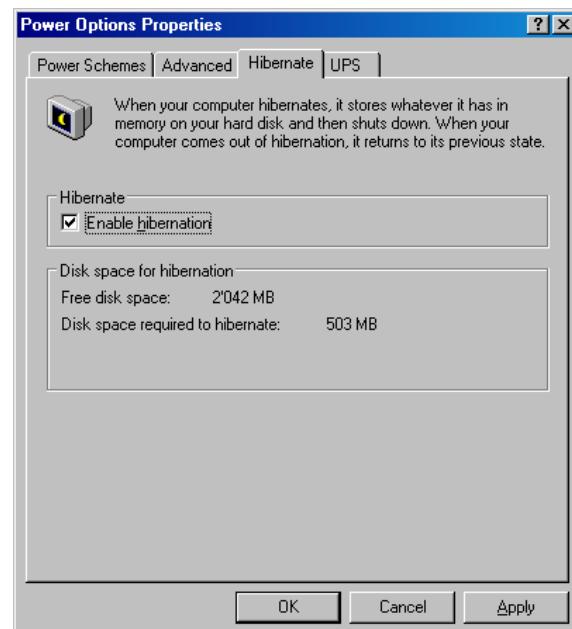
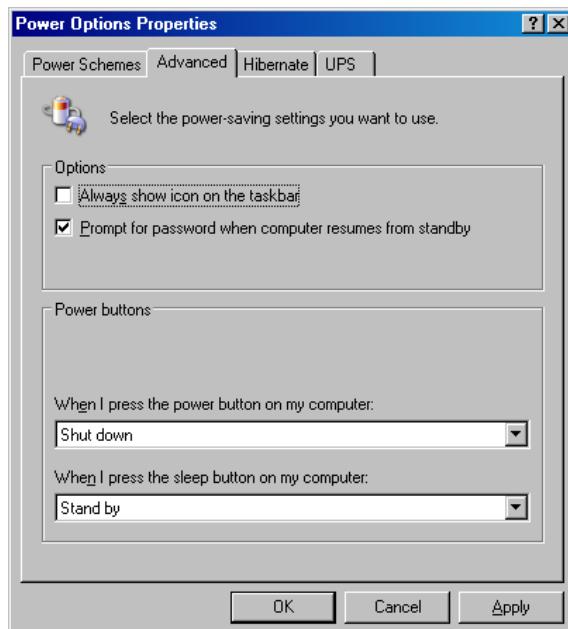
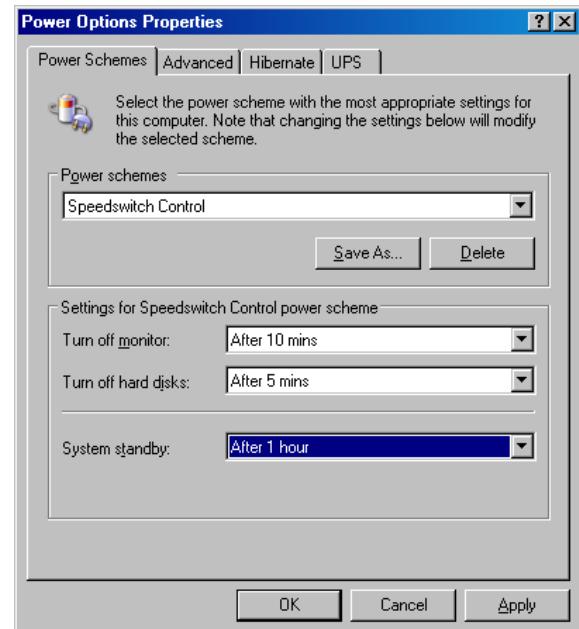
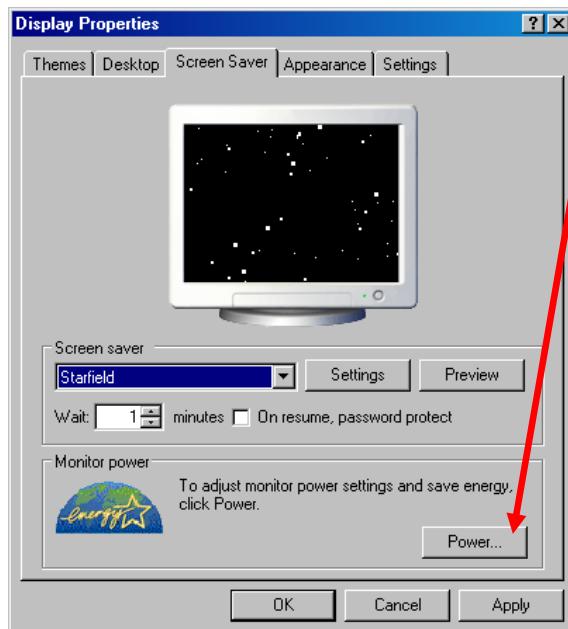
Windows XP Power Schemes	AC Power (Frequency example: mobile Pentium-M 2 GHz)	Battery DC (Frequency example: mobile Pentium-M 1.6 GHz)
Home/Office Desktop	None (2 GHz Always)	Adaptive (600 MHz <...>1.6 GHz)
Portable/Laptop	Adaptive (800 MHz <...>2 GHz)	Adaptive (600 MHz <...>1.6 GHz)
Presentation	Adaptive (800 MHz <...>2 GHz)	Degrade (600 MHz)
Always On	None (2 GHz Always)	None (1.6 GHz Always)
Minimal Power Management	Adaptive (800 MHz <...>2 GHz)	Adaptive (600 MHz <...>1.6 GHz)
Maximum Battery	Adaptive (800 MHz <...>2 GHz)	Degrade (600 MHz)

CPU performance is heavily dependent on the choice of power scheme in the system control.

4.5.1 Set up Power Management

Start / Control Panel / Appearance and Themes / Display Properties / Screen Saver tab

Enter the following settings: click the "Power..." button



5 The Special Function Interface (SFI)

All functions are performed by starting the SW Interrupt 15hex with the following arguments:

5.1 INT15h SFR Functions

Function	WRITE TO EEPROM		
Number	E0h		
Description			Writes the data byte into the addressed User-Memory-Cell from the serial EEPROM. The old value is automatically deleted.
Input values	AH	78h	DLAG Int15 function
	AL	E0h	Function request
	BX		Address in the EEPROM (0-1024 possible)
	CL		Data byte to store
	SI		1234h User-Password (otherwise EEP is write-protected)
Output value			None, all registers are restored when reopened.

Function	READ FROM EEPROM		
Number	E1h		
Description			Reads the data byte into the addressed User-Memory-Cell of the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	E1h	Function request
	BX		Address in the EEPROM (0-1024 possible)
	SI		1234h User-Password (DLAG-Password for access to the DLAG-Memory-Cells)
Output value	AL		Data byte

Function	WRITE SERIAL NUMBER		
Number	E2h		
Description			Writes the serial number from the serial EEPROM into the addressed DLAG-Memory-Cell. The old value is automatically deleted.
Input values	AH	78h	DLAG Int15 function
	AL	E2h	Function request
	BX, CX, DX		Serial number
	SI		Password
Output value			None, all registers are restored when reopened.

Function	READ SERIAL NUMBER		
Number	E3h		
Description			Reads the serial number from the board into the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	E3h	Function request
Output values	BX, CX, DX		Serial number (binary, not ASCII)

Function	WRITE PRODUCTION DATE		
Number	E4h		
Description			Writes the production date into the addressed DLAG-Memory-Cell from the serial EEPROM. The old value is automatically deleted. If the password is also in DX, the counters will be reset (=0).
Input values	AH	78h	DLAG Int15 function
	AL	E4h	Function request
	BX, CX		Production date
	CL		Day of month (1-31)
	DI		Password (clear counter)
	SI		Password
Output value			None, all registers are restored when reopened.

Function	READ PRODUCTION DATE		
Number	E5h		
Description			Reads the production date from the board in the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	E5h	Function request
Output values	BX, CX		Production date

Function	WRITE INFO 2 TO THE EEPROM		
Number	E8h		
Description			Writes the information bytes into the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	E8h	Function request
	SI		Password
	DI		CPU type bits 1-7 and board type bits 8-15. CPU type: 01h=ELAN300/310, 02h=ELAN400, 05h=P5, 08h=P3, 09h=ELAN520, 10h=P-M / BOARD TYPE ('M'=PC/104, 'E'=Euro, 'W'=MSWS, 'S'=Slot, 'C'=Custom, 'X'= smartCore or smartModule)
	BH, BL		Board version (i.e., V1.5 → BH=1, BL=5)
	CH, CL		BIOS version (i.e., V3.0 → CH=3, CL=0)
	DH		Number of 512K FLASH
	DL		Number of 512K SRAM
			None, all registers are restored when reopened.

Function	READ INFO 2 FROM THE EEPROM		
Number	E9h		
Description			Reads the information bytes out of the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	E9h	Function request
Output values	AL		Board type BOARD TYPE ('M'=PC/104, 'E'=Euro, 'W'=MSWS, 'S'=Slot, 'C'=Custom, 'X'= smartCore or smartModule)
	DI		CPU type bits 1-7 and board type bits 8-15. CPU type: 01h=ELAN300/310, 02h=ELAN400, 05h=P5, 08h=P3, 09h=ELAN520, 10h=P-M / BOARD TYPE ('M'=PC/104, 'E'=Euro, 'W'=MSWS, 'S'=Slot, 'C'=Custom, 'X'= smartCore or smartModule)
	BH, BL		Board version (i.e., V1.5 → BH=1, BL=5)
	CH, CL		BIOS version (i.e., V3.0 → CH=3, CL=0)
	DH		Number of 512K FLASH
	DL		Number of 512K SRAM

Function	READ INFO 3 FROM THE EEPROM (READ COUNTER – LOW 2 BYTE OF 3 BYTE COUNTER)		
Number	EAh		
Description			Reads the information bytes out of the serial EEPROM.
Input values	AH	78h	DLAG Int15 function
	AL	EAh	Function request
Output values	AX		Number of boot errors
	BX		Number of setup entries
	CX		Number of low battery errors
	DX		Number of power-on starts

Function	WATCHDOG		
Number	EBh		
Description			Enables strobes and disables the Watchdog. After power-up, the Watchdog is always disabled. Once the Watchdog has been enabled, the user application must perform a strobe at least every 800ms, otherwise the Watchdog performs a hardware reset.
Input values	AH	78h	DLAG Int15 function
	AL	EBh	Function request
	BL	00h	Disable
	BL	01h	Enable
	BL	FFh	Strobe
	BH		00h=BL → number of seconds / 01h=BL → number of minutes
Output value	AL	01h	Watchdog timer time-out occurred.

Function	READ TEMPERATURE OF THE CPU		
Number	ECh		
Description			Reads the temperature from the LM75 or CPU thermal sensor.
Input values	AH	78h	DLAG Int15 function
	AL	ECh	Function request
Output values	BL		00h → value OK, otherwise error
	CL		ADM1023 temp bit 7=01h neg./*1C
	DX		CPU temp (from the ADM1023) bit 10=01h neg./*0125C

5.2 Int15 Emulator Driver for Windows

5.2.1 Int15 Hardware

Resources:

1. EEPROM: 2K size
000h-3FFh: reserved
400h-7FFh: available for user data
2. Temperature sensor
3. Watchdog hardware

Access to these resources under DOS can be provided by INT 15h function, see Section 6.1.

Access under Windows 98, ME, 2000 and XP can be provided by the "Int15dl"-WDM driver; under Windows-NT with the "Int15dl"-NT driver.

At the moment this driver supports all Kontron Compact Computers' boards with PIIX4 and ICH4 chipsets (e.g., MSM855, MSEBX855, MSMP5SEV, MSMP3SEV, MSEP800, etc.).

You'll find the driver under: x:\tools\int15dl\... on the Product CD or in the download area of the support center.

5.2.2 Int15 Windows Software

- » WinInt15.exe (Int15 function test tool)
- » T945.exe (Temperature sensor [SMBUS] monitor)

5.2.3 Driver Installation W2k/XP

"Int15dl" is not a plug-and-play driver, it must be installed manually:

1. Open "Control Panel".
2. Double click on "Add/Remove Hardware".
3. To continue click the "Next>" button.
4. On the page "Choose a Hardware Task", check "Add/Troubleshoot a device" and click "Next>".
5. After "New hardware detection", an automatic Windows procedure, choose "Add a new device" item and click the "Next>" button.
6. On the "Find New Hardware" page, choose "No, I want to select the hardware from a list" and click "Next>".
7. Choose "Other devices" in the "Hardware Type" list and click the "Next>" button.
8. On the page "Select a Device Driver" press the "Have Disk..." button and find the driver location (Int15dl.inf-WDM). After opening the "inf" file, the installation program will show a Models list and "DIGITAL-LOGIC INT15 functions emulator" string. Press the "Next>" button.
9. Then press the "Finish" button. It is not necessary to restart the computer after installation.
10. After installation, please, be sure, that "DIGITAL-LOGIC INT15 functions emulator" has been installed properly. Open "Control Panel", then double click on the "System" icon. Choose the "Hardware" tab and click on the "Device Manager" button. Expand "System Devices" and double click on "DIGITAL-LOGIC INT15 functions emulator". Be sure that device is working properly.

5.2.4 Driver Installation Windows-NT

1. Boot with administrative privileges.
2. Copy NT-driver "Int15dl.sys" into WINNT\System32\drivers folder.
3. Register the driver by double clicking on the "int15dl.reg" file.
4. Reboot the computer.

5.2.5 Programming Int15dl Interface under Windows

Programming of the Int15dl interface is very similar to DOS programming and is based on the DeviceIO control function, which operates with a pre-defined structure named "Registers".

Files:

Int15srv.h: contains definitions for the Registers structure.
 Int15dlioclt.h: contains definitions for the IO control code constants.
 Test_Int15dl.cpp: sample subroutines providing access to hardware functions over the Int15dl driver

Functions (Test_Int15dl.cpp)

bool Int15(Registers *Regs): the main function, which sends user requests to the driver.

Returns **true** if the request finished successfully, otherwise it returns **false**.

Regs: address of the Registers structure containing specific request data (defined in Int15srv.h).

For example, the following code will initiate temperature measuring:

```
Registers Regs;
Regs.ah = 0xEC;
if(!Int15(&Regs)) //error in driver request
{
    printf("Error reading temperature\n");
    return;
}
//success - temperature value is in Regs.al
if(Regs.bl == 0)printf("\tTemperature = %d C\n",Regs.al);
//error - not valid value
else printf("\tError reading Temperature\n");
```

Note: Input and output arguments of the Int15 function differ for the various chipsets and BIOSes. Read about the Registers definition in the user manual.

For example: To get temperature value on a board with the PIIX4 chipset, use "Regs.ah = 0xEC;" on a board with the ICH4 chipset, use "Regs.ax = 0x78EC;".

bool Open_Int15dl(void): the first function and must be called to create a link between the "DIGITAL-LOGIC INT15 functions emulator" driver and the user software.

Returns **true** if the device was successfully opened, otherwise it returns **false**.

void Close_Int15dl(void): the last function; it breaks the link between the driver and user software.

int GetChipID(void): an additional service function; returns the type of chipset (for PIIX4 = 4, for ICH4 = 5).

Registers Structure

This is used for exchanging information between the user program and the "Int15dl" driver.

```
typedef struct Registers {
    union {
        struct {
            unsigned short ax;
            unsigned short bx;
            unsigned short cx;
            unsigned short dx;
            unsigned short bp;
            unsigned short si;
            unsigned short di;
            unsigned short ds;
            unsigned short es;
            unsigned short flags;
        };
        struct {
            unsigned char al;
            unsigned char ah;
            unsigned char bl;
            unsigned char bh;
            unsigned char cl;
            unsigned char ch;
            unsigned char dl;
            unsigned char dh;
        };
    };
} TRegisters;
```

Information for Advanced Users

At the first call of the function **Open_Int15dl()**, the Int15dl driver tries to detect the type of chipset. To disable this procedure the user must define the following parameters in the "Int15dl.inf" file before installation of the driver:

For PIIX4 chipset:

```
HKR, "Parameters", "chipID", 0x00010001, 0x4
HKR, "Parameters", "pmBase", 0x00010001, 0x1000
HKR, "Parameters", "smbBase", 0x00010001, 0x1040
HKR, "Parameters", "tsaddr", 0x00010001, 0x9E - LM75 sensor address
```

For ICH4 chipset:

```
HKR, "Parameters", "chipID", 0x00010001, 0x5
HKR, "Parameters", "pmBase", 0x00010001, 0x1000
HKR, "Parameters", "smbBase", 0x00010001, 0x1880
HKR, "Parameters", "tsaddr", 0x00010001, 0x9C - ADM1023 sensor address
```

For more information, please get in contact with the Kontron Compact Computers support department.

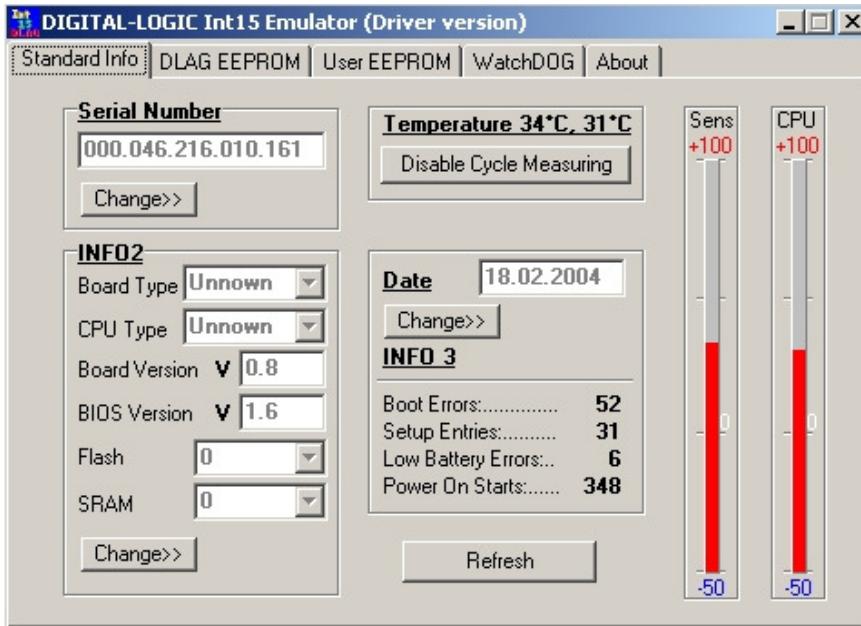
6 Software

6.1 Windows Int15 Tool

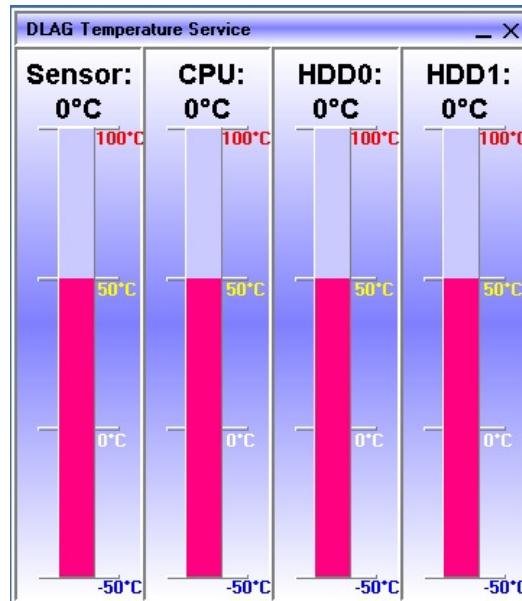
The tool and driver are on the Product CD under: x:\tools\int15dl\... or in the download area of the support center.

6.2 Int15 Windows Software

WinInt15.exe (Int15 function test tool)



T945.exe (Temperature sensor [SMBUS] monitor)



7 Diagnostics

7.1 Phoenix SecureCore™ Checkpoint Lists for the SMA200

7.1.1 POST Code Checkpoints

The POST code checkpoints are the largest set of checkpoints during the BIOS pre-boot process. The following table describes the type of checkpoints that may occur during the POST portion of the BIOS

Note: Checkpoints may differ between different platforms based on system configuration.
Checkpoints may change due to vendor requirements, system chipset or optional ROMs from add-in PCI devices.

Code	Beeps	POST Routine Description
02h		Verify Real Mode
03h		Disable Non-Maskable Interrupt (NMI)
04h		Get CPU type
06h		Initialize system hardware
07h		Disable shadow and execute code from the ROM.
08h		Initialize chipset with initial POST values
09h		Set IN POST flag
0Ah		Initialize CPU registers
0Bh		Enable CPU cache
0Ch		Initialize caches to initial POST values
0Eh		Initialize I/O component
0Fh		Initialize the local bus IDE
10h		Initialize Power Management
11h		Load alternate registers with initial POST valuesnew
12h		Restore CPU control word during warm boot
13h		Initialize PCI Bus Mastering devices
14h		Initialize keyboard controller
16h	1-2-2-3	BIOS ROM checksum
17h		Initialize cache before memory Autosize
18h		8254 timer initialization
1Ah		8237 DMA controller initialization
1Ch		Reset Programmable Interrupt Controller
20h	1-3-1-1	Test DRAM refresh
22h	1-3-1-3	Test 8742 Keyboard Controller
24h		Set ES segment register to 4GB
28h		Autosize DRAM
29h		Initialize POST Memory Manager
2Ah		Clear 512kB base RAM
2Ch	1-3-4-1	RAM failure on address line xxxx*
2Eh	1-3-4-3	RAM failure on data bits xxxx* of low byte of memory bus
2Fh		Enable cache before system BIOS shadow
32h		Test CPU bus-clock frequency
33h		Initialize Phoenix Dispatch Manager
36h		Warm start shut down
38h		Shadow system BIOS ROM
3Ah		Autosize cache
3Ch		Advanced configuration of chipset registers
3Dh		Load alternate registers with CMOS valuesnew
41h		Initialize extended memory for ROM Pilot
42h		Initialize interrupt vectors
45h		POST device initialization
46h	2-1-2-3	Check ROM copyright notice
47h		Initialize I2O support
48h		Check video configuration against CMOS
49h		Initialize PCI bus and devices
4Ah		Initialize all video adapters in system

Code	Beeps	POST Routine Description
4Bh		QuietBoot start (optional)
4Ch		Shadow video BIOS ROM
4Eh		Display BIOS copyright notice
4Fh		Initialize MultiBoot
50h		Display CPU type and speed
51h		Initialize EISA board
52h		Test keyboard
54h		Set key click if enabled
55h		Enable USB devices
58h	2-2-3-1	Test for unexpected interrupts
59h		Initialize POST display service
5Ah		Display prompt "Press F2 to enter SETUP"
5Bh		Disable CPU cache
5Ch		Test RAM between 512 and 640kB
60h		Test extended memory
62h		Test extended memory address lines
64h		Jump to UserPatch1
66h		Configure advanced cache registers
67h		Initialize Multi Processor APIC
68h		Enable external and CPU caches
69h		Setup System Management Mode (SMM) area
6Ah		Display external L2 cache size
6Bh		Load custom defaults (optional)
6Ch		Display shadow-area message
6Eh		Display possible high address for UMB recovery
70h		Display error messages
72h		Check for configuration errors
76h		Check for keyboard errors
7Ch		Set up hardware interrupt vectors
7Dh		Initialize Intelligent System Monitoring
7Eh		Initialize coprocessor if present
80h		Disable onboard Super I/O ports and IRQs
81h		Late POST device initialization
82h		Detect and install external RS232 ports
83h		Configure non-MCD IDE controllers
84h		Detect and install external parallel ports
85h		Initialize PC-compatible PnP ISA devices
86h		Re-initialize onboard I/O ports
87h		Configure Motherboard Configurable Devices (optional)
88h		Initialize BIOS Data Area
89h		Enable Non-Maskable Interrupts (NMIs)
8Ah		Initialize Extended BIOS Data Area
8Bh		Test and initialize PS/2 mouse
8Ch		Initialize floppy controller
8Fh		Determine number of ATA drives (optional)
90h		Initialize hard disk controllers
91h		Initialize local-bus hard disk controllers
92h		Jump to UserPatch2
93h		Build MPTABLE for multi-processor boards
95h		Install CD ROM for boot
96h		Clear huge ES segment register
97h		Fix up Multi Processor table
98h	1-2	Search for option ROMs. One long, two short beeps on checksum failure
99h		Check for SMART Drive (optional)
9Ah		Shadow option ROMs
9Ch		Set up Power Management
9Dh		Initialize security engine (optional)
9Eh		Enable hardware interrupts
9Fh		Determine number of ATA and SCSI drives
A0h		Set time of day
A2h		Check key lock
A4h		Initialize typematic rate
A8h		Erase F2 prompt
AAh		Scan for F2 key stroke

Code	Beeps	POST Routine Description
ACh		Enter SETUP
AEh		Clear Boot flag
B0h		Check for errors
B1h		Inform RomPilot about the end of POST
B2h		POST done – prepare to boot operating system
B4h	1	One short beep before boot
B5h		Terminate QuietBoot (optional)
B6h		Check password (optional)
B7h		Initialize ACPI BIOS
B9h		Prepare Boot
BAh		Initialize SMBIOS
BBh		Initialize PnP Option ROMs
BCh		Clear parity checkers
BDh		Display MultiBoot menu
BEh		Clear screen (optional)
BFh		Check virus and backup reminders
C0h		Try to boot with INT 19
C1h		Initialize POST Error Manager (PEM)
C2h		Initialize error logging
C3h		Initialize error display function
C4h		Initialize system error handler
C5h		PnPd dual CMOS (optional)
C6h		Initialize note dock (optional)
C7h		Initialize note dock late
C8h		Force check (optional)
C9h		Extended checksum (optional)
CAh		Redirect Int 15h to enable remote keyboard
CBh		Redirect Int 13h to Memory Technologies Devices such as ROM, RAM, PCMCIA, and serial disk
CCh		Redirect Int 10h to enable remote serial video
CDh		Remap I/O and memory for PCMCIA
CEh		Initialize digitizer and display message
D2h		Unknown interrupt

The following are for Boot Block in the Flash ROM:

Code	Beeps	POST Routine Description
E0h		Initialize the chipset
E1h		Initialize the bridge
E2h		Initialize the CPU
E3h		Initialize system timer
E4h		Initialize system I/O
E5h		Check force recovery boot
E6h		Checksum BIOS ROM
E7h		Go to BIOS
E8h		Set Huge Segment
E9h		Initialize Multi Processor
EAh		Initialize OEM special code
EBh		Initialize PIC and DMA
EC _h		Initialize Memory type
EDh		Initialize Memory size
EEh		Shadow Boot Block
EFh		System memory test
F0h		Initialize interrupt vectors
F1h		Initialize Run Time Clock
F2h		Initialize video
F3h		Initialize System Management Manager
F4h		Output one beep
F5h		Boot to Mini DOS
F6h		Clear Huge Segment
F7h		Boot to Full DOS

8 BIOS

8.1 BIOS History

Vers.	Date	Status	Edited by	Modifications
0.01-0.18	17.06.2008 - 01.03.2009	Development	BRM/VIV	Pre-release development of the BIOS
1.00	12.03.2009	Released	BRM/VIV	BIOS released
1.01	14.04.2009	"	BRM/VIV	Programming of Fintek
1.02	17.04.2009	"	BRM/VIV	ALC882 audio codec definition
1.03	28.05.2009	Released	BRM/VIV	Floppy controller disabled/Memory detection fixed/Firmware version visible in BIOS setup
1.04	02.06.2009	"	BRM	Fix for Fintek LPC UART
1.05	01.07.2009	"	BRM	USB client fix
1.06	21.07.2009	Released	BRM	Fix of diagnostic screen & SuperIO address 200h
1.07	13.08.2009	"	BRM/VIV	Fix of pcirst & audio for MID platform/New PCIe bus enumeration
1.08	24.08.2009	"	BRM	IRQExclude menu added for LPC/ISA IRQ reservation
1.09	27.08.2009	Released	BRM	New microcode from Intel Rev. 217h
1.10	28.08.2009	"	BRM	ACPI fix for PNP OS (PCI routing)
1.11	31.08.2009	"	VIV	BIOS for MPCX28 can be used as standard/Tests for FPGA presence
1.12	14.09.2009	Released	VIV	Wake-up from PS2 KB/MS from S3 state
1.13	03.11.2009	"	BRM	Fix of COM1&2 swap with COM3&4/PCIe fix
1.14	12.11.2009	"	BRM	New Poulsbo firmware
1.15_GTL	03.12.2009	Released	BRM	C6 split VTT disabled
1.16_GTL	06.01.2010	"	BRM/VIV	ASPM default set to disabled/sbinit.asm updated/Save-Restore FPGA & F81216 content for S3 stated added
1.17_GTL	07.01.2010	"	VIV	GPIO7 output changed to fixed "1" disabling C6 control/Bootblock
1.18_GTL	13.01.2010	Released	BRM	Splash screen changed (Kontron was not black)
1.19_GTL	08.02.2010	"	BRM	Switched to 1.5V DDR2 voltage in Poulsbo firmware
1.20_GTL	11.03.2010	"	VIV	Fix in ACPI-COM ports from Fintek detection.
1.21_GTL	16.03.2010	Released	BRM	DMI info updated to Kontron/Serial port of IRQ of COM5 (Fintek) corrected to IRQ5
1.22_GTL	20.04.2010	"	VIV	Implemented Kontron DMI info
1.23_GTL	29.04.2010	"	BRM	New SATA boot ext. V7.7.0.2/Fix for USB KB on USB controller 1
1.24_GTL	03.05.2010	Released	BRM	SATA boot ext. V7.4.0.5 for Windows XP compatibility
1.25_GTL	23.09.2010 05.10.2010	"	VIV	FPGA index changed to 0 at end of FPGA watchdog initialization/Content of WD added (for save-restore from S3 state) Universal version for SMA200 and MPCX28
1.26_GTL	08.10.2010	"	BRM	Azalia codec table for Realtek added

8.2 Specifications of the BIOS

Embedded BIOS	Remarks
ACPI PM	V3.0 Power Management
ACPI Battery Support	Not enabled
Boot Devices	PATA, SATA, USB-Devices, LAN
CMOS-Data	Battery backed SRAM and a copy in the EEPROM
BIOS Setup Backup	Automatically written into the EEPROM after setup-screen exit
Battery-less Boot	Generally possible, setup data are transferred from the EEPROM. The system integrator is responsible for testing and validating the application software on a battery-less platform. Without backup-battery, the time and date counter is not running while the computer system is switched off!
Customized CMOS	Possible, must be ordered separately
Customized User Data	Possible, must be ordered separately
PCI Parallel	Supports PCI V2.2 with up to 6 resources
PCIexpress	Supports PCI V2.2
TPM V1.2	Trusted Platform Module, optionally connectable to the SMB-Bus
Watchdog Support	Shutdown or restart, depends on the implementation
RAID Support	No
IDE Mode	Compatible mode (IRQ14/15) or Native mode (PCI device)
APIC-Support	Yes, Advanced Programmable Interrupt Controller
AHCI	No
EIST	Yes, Enhanced Intel SpeedStep Technology
Intel 64	No
Intel VT	Z530 only
Thermal Management	Yes, integrated in the ACPI Throttling processor function Control of the fan for active cooling Critical trip point (the OS must shut down the system asap) Catastrophic temperature (hardware shutdown)
Supported ACPI Suspend Modes	Supported are: S1 (POS = Power On Suspend) S3 (STR = Suspend to RAM) S4 (Suspend to Disk) is not supported by the BIOS; alternatively, the Win2000 and Win XP Operating Systems use S4-OS (Hibernate)

Wakeup Events	Remarks
Power Button	Wakes unconditionally from S1-S5
GPI1#	Only if configured as LID Switch
GPI2#	Only if configured as RESUME ON RING
WOL, LAN wake event	LAN driver must be configured for WOL
SMBALERT#	Wakes up unconditionally from S1-S5
PCIexpress WAKE#	Wakes up unconditionally from S1-S5
PME#	Activates the wake-up capabilities of a PCI-circuit
USB Mouse/KB	When standby mode S1 is set, the wake-up with USB MS/KB works. This depends on the system implementations.

8.3 Core BIOS Functions

INTEL Chipset Support US15W	Remarks
US15W Support with all timings (DDRAM , ...)	Auto-detect PCI/internal video in the US15W. Internal video BIOS only if no PCI available.

Password/Security	Remarks
Standard functions	
TCP/IP number for FirstWare tools	(browser, download service)

Multi-boot Setup	Remarks
Boot from FD	
Boot from HD	
Boot from CD	
Boot from USB FD	
Boot from USB CD	
Boot from LAN	INTEL 82574L

Serial Remote Console Function	Remarks
Enable/Disable/Auto-detect	Select COM1 or COM2

LPC-Setup (LPC-SuperIO W83627HF)	Remarks
COM1	IRQ selection
COM2	IRQ selection
FD (and IRQ6)	Enable/disable
LPT (and IRQ7)	Enable/disable
PS/2-Keyboard (and IRQ1)	Enable/disable
PS/2-MS (and IRQ12)	Enable/disable
IRQ definitions	PnP, PCI, ISA

Keyboard Settings	Remarks
Standard-like	Typematic rate, numlock status, ...

Power Management	Remarks
ACPI Functions	
APM Function	
AC-Full speed CPU Frequency select	
Battery-Speed CPU Frequency select	
Trottle temperature	
Trottle function	
Other thermal protection features of the PENTIUM-M	
Wake on LAN	Enable/disable, setting of the TCP/IP number
Suspend to RAM (S3)	Planned
Suspend to Disk (S4)	
Communication over SMB with the PIC-PM-Controller for Wake-up/Suspend	
AC-Detect for full speed	No AC means battery-mode speed

Wake Events	Remarks
LAN activity	
KB activity	
MS activity	
Active ring signal	
PWRBTN#	AVR Microcontroller

Suspend Events	Remarks
PWRBTN# (S2R or S2D)	AVR Microcontroller
No activity over a defined time	Select time from 1-255 minutes
Software controlled shutdown	
Smart Battery down	0%, 5%, 10%, 15%, 20%, off (SMB-detect of LTC1779)
Time-controlled suspend	

Fast Boot	Remarks
Normal	15-25sec = normal boot
Fast boot	10-15sec = quick boot
Failure activity	No-Wait, Wait and error display, No-Wait and counter in the EEPROM
Boot counter	Enable/disable (in the EEPROM)

Screen	Remarks
Boot-up screen	CRT (SDVO) ,LVDS
Start-up resolution in the BIOS	640x480, 600x800, 1024x768
Boot-up logo	Enable/disable

For Realtime Operating Systems	Remarks
HotPlug-Service	Enable/disable
USB-HotPlug Service	Enable/disable

Battery-less BIOS-Setup	Remarks
Automatic save/reload of the EEPROM values	If battery fails
INT15 services	

Download Functions	Remarks
CoreBIOS download	DOS / Windows

Watchdog (planned)	Remarks
Watchdog	Enable/disable
Time out	1, 10, 20, 30, 40, 50, 60 sec, 2, 3, 4, 5-32min

8.4 Core BIOS Download

Before downloading a BIOS, please check the following:

Make a bootable diskette which includes the following files:

- » DELEP200.exe
- » Phlash16.exe
- » core BIOS (SM200_xxx_FLASHABL.ROM)

Rename the SM200_xxx_FLASHABL.ROM file to bios.rom

IMPORTANT: Do not use boot disks created in a Windows operating system. If you do not have an MSDOS 6.22 disk available, you can download a boot disk from www.bootdisk.com.

Notes:

- ▶ Disable the EMM386 or other memory managers in the CONFIG.SYS of your bootdisk.
- ▶ Make sure that the PHLASH16.exe program and the BIOS to be downloaded are in the same path and directory!
- ▶ Boot DOS without config.sys and autoexec.bat → press **F5** while starting the DOS boot.
- ▶ Is the empty disk space, where the PHLASH16.exe is located, larger than 64kB (for safe storage)?
- ▶ Is the floppy disk not write-protected?

Start the DOWNLOADING process:

1. Start the system with the bootable diskette. If you do not have a bootable diskette or floppy drive you can start in DOS mode by pressing the F5 key to disable the autoexec.bat and config.sys.
2. Run DELEP200.exe to clear the CMOS and the EEPROM.

Warning If you do not run DELEP200.exe, the system will be destroyed during the BIOS upgrade!

3. Run **PHLASH16.EXE BIOS.ROM /BBL**
4. If the BIOS download is finished, you must power off the system.
5. After powering the system back on, press **F2** to enter the setup mode and set the default values with **F9**.
6. "Save and leave" the setup with **F10**.
7. Power off the system.
8. The download procedure is finished.

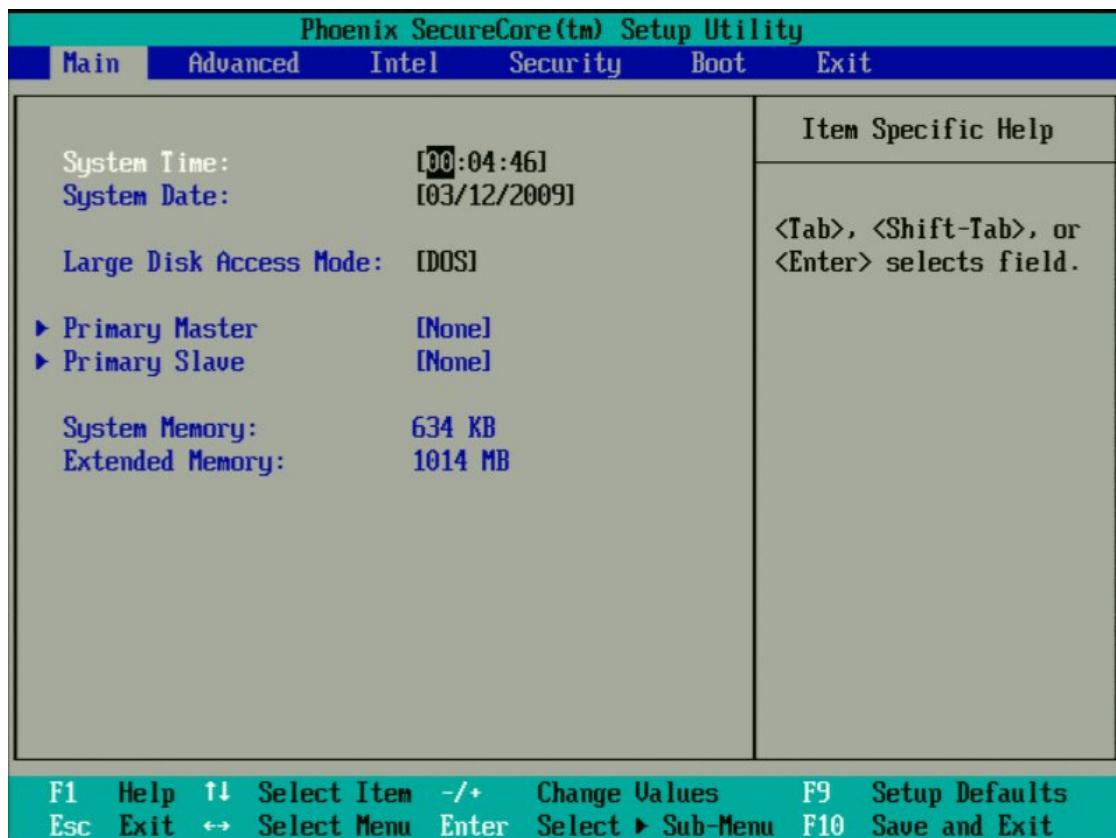
8.5 BIOS Setup

Setup Menu Screens and Navigation

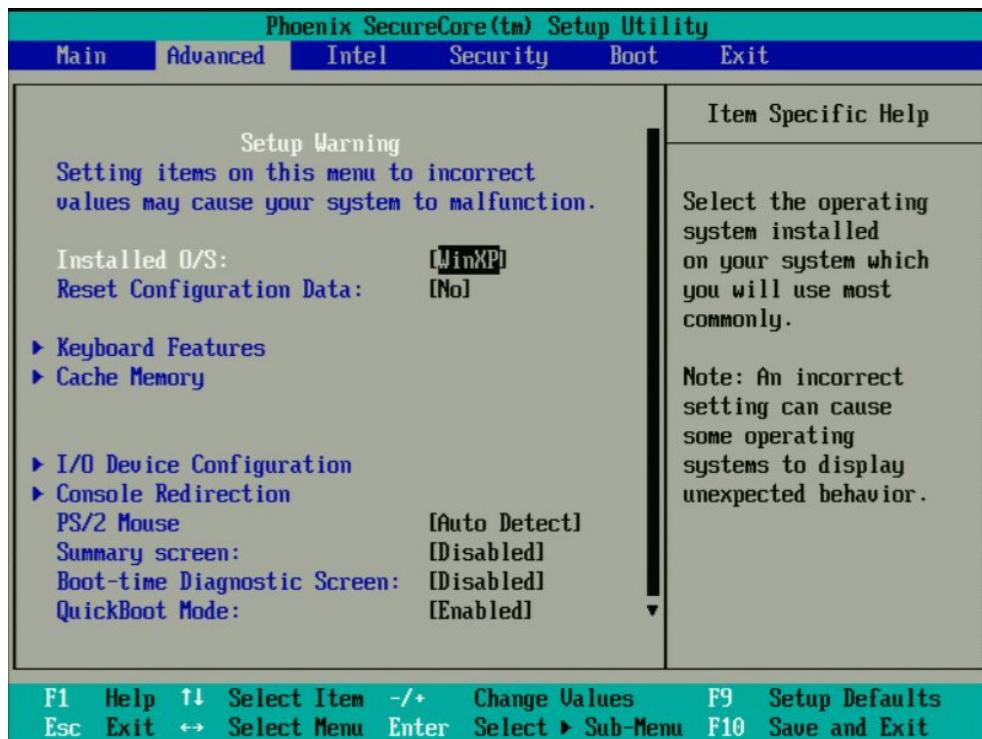
Keystroke Controls:

Function	Key
Enter Setup	F2
Pop-up Boot Menu	ESC

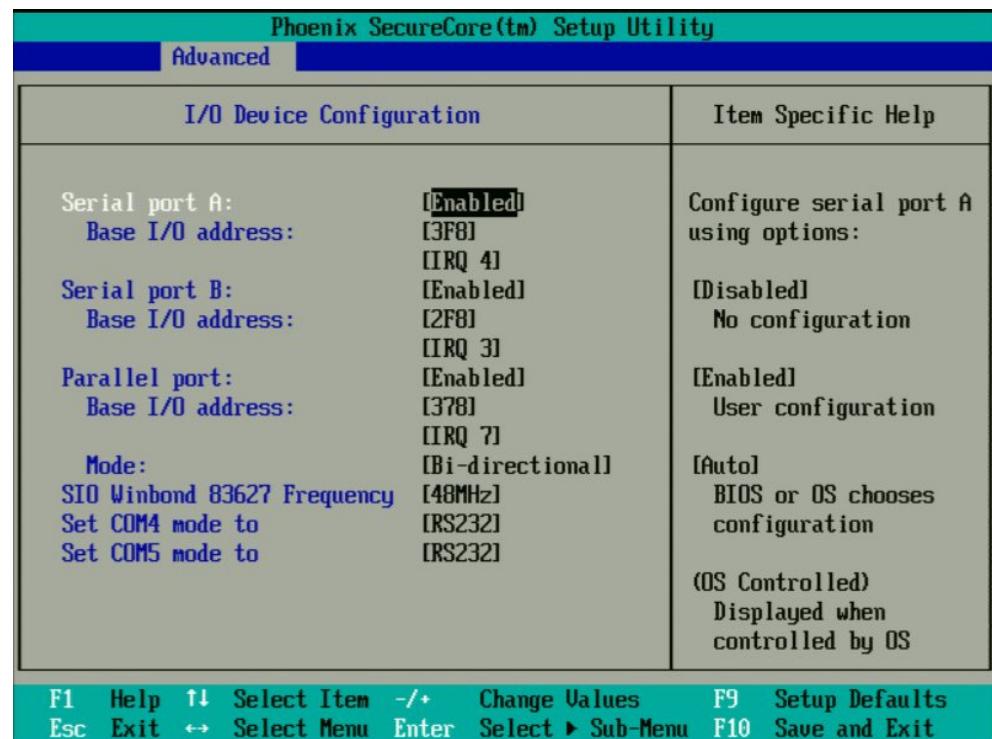
8.5.1 Main Menu



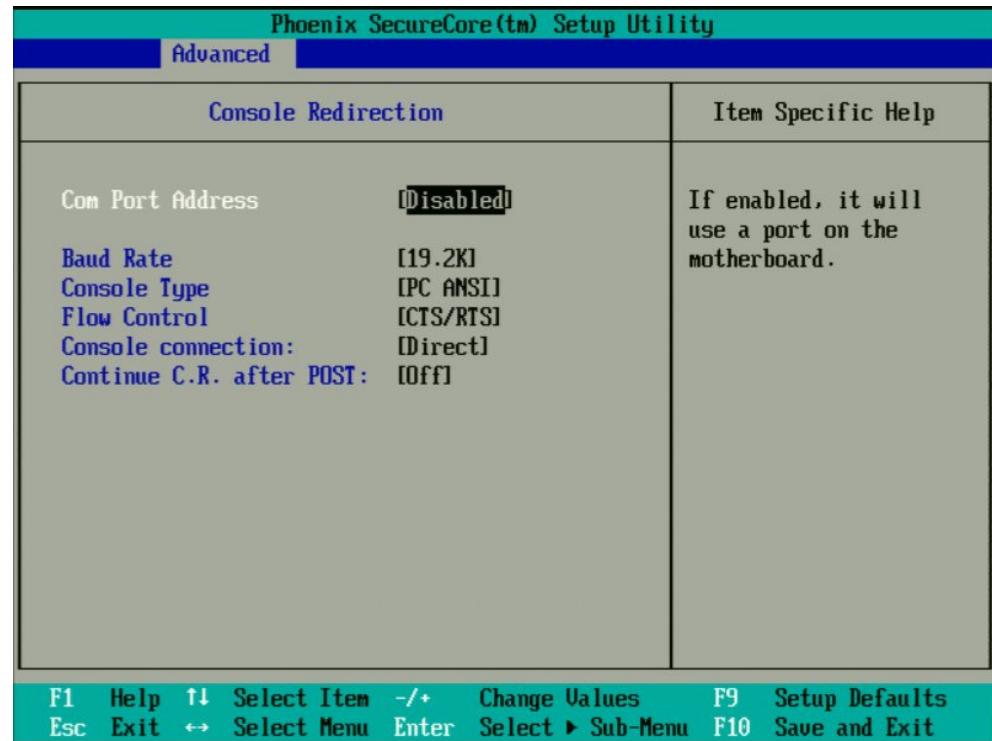
8.5.2 Advanced



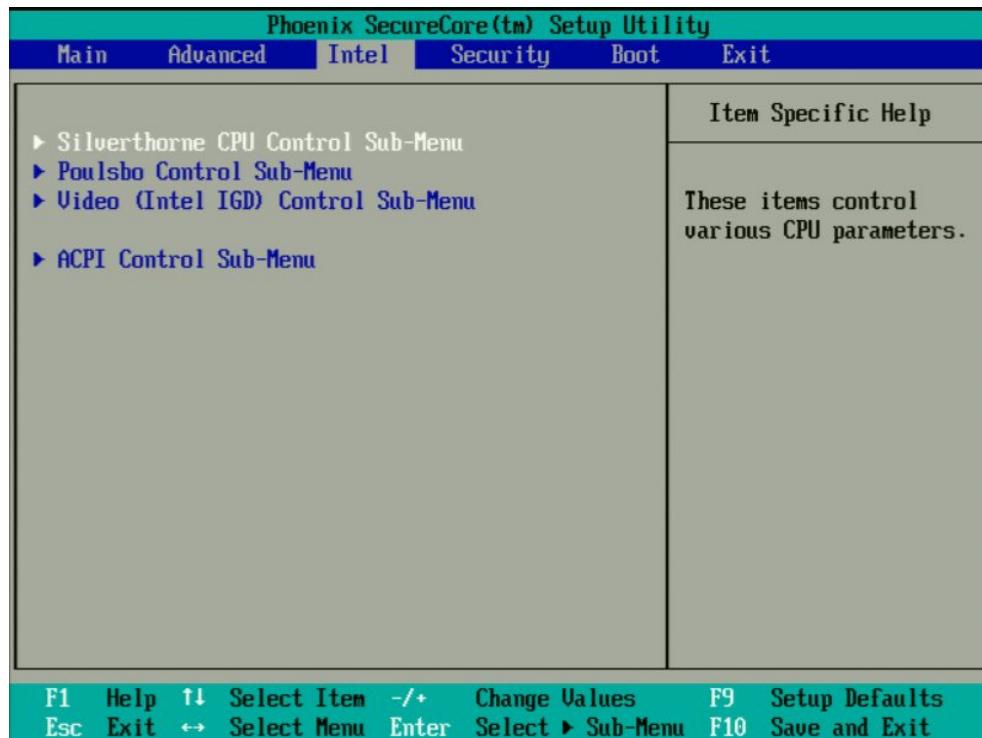
8.5.3 Advanced I/O Configuration



8.5.4 Advanced Console Redirection



8.5.5 Intel



8.5.6 Intel CPU Control

Phoenix SecureCore(tm) Setup Utility	
Intel	
Silverthorne CPU Control Sub-Menu	Item Specific Help
Hyperthreading: [Enabled]	Enabling Hyperthreading activates additional CPU threads. These threads may appear as additional processors but will share some resources with the other threads within the physical package.
Processor Power Management: [GU3 Only]	
▶ CPU Thermal Control Sub-Menu	
No Execute Mode Mem Protection [Enabled]	
Intel(R) Virtualization Technology [Enabled]	
Set Max Ext CPUID = 3 [Disabled]	

F1 Help $\uparrow\downarrow$ Select Item $-/+$ Change Values F9 Setup Defaults
 Esc Exit \leftrightarrow Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

8.5.7 Intel CPU Thermal Control

Phoenix SecureCore(tm) Setup Utility	
Intel	
CPU Thermal Control Sub-Menu	Item Specific Help
Thermal Control Circuit: [TM2]	Setting this bit enables the thermal control circuit (TCC) portion of the Thermal Monitor feature of the CPU.
PROCHOT# Enable: [Enabled]	
DTS Enable: [Disabled]	
Thermal Monitor Enable: [Disabled]	
Active Trip Point: [55 C]	Intel(r) Thermal Monitor TM1 = 50% duty cycle
Passive Cooling Trip Point: [95 C]	TM2 = Geyserville III
Passive TC1 Value: [0]	
Passive TC2 Value: [10]	
Passive TSP Value: [2]	
Critical Trip Point: [POR]	

F1 Help $\uparrow\downarrow$ Select Item $-/+$ Change Values F9 Setup Defaults
 Esc Exit \leftrightarrow Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

8.5.8 Intel Poulsbo Control

Phoenix SecureCore(tm) Setup Utility	
Intel	
Poulsbo Control Sub-Menu	Item Specific Help
▶ PCI Express Control Sub-Menu	
▶ Poulsbo USB Control Sub-Menu	
Azalia - Device 27, Function 0: [Auto]	
SDIO - Device 30, Function 0/1/2: [Disabled]	
SATA OROM: [Enabled]	
PXE OROM: [Disabled]	
PCI Clock Run: [Enabled]	
Serial IRQ Quiet Mode: [Disabled]	
Pop Up Mode Enable: [Enabled]	
Pop Down Mode Enable: [Enabled]	

F1 Help **↑↓** Select Item **-/+** Change Values F9 Setup Defaults
 Esc Exit **↔** Select Menu Enter Select **▶** Sub-Menu F10 Save and Exit

8.5.9 Intel Poulsbo PCI Express Control

Phoenix SecureCore(tm) Setup Utility	
Intel	
PCI Express Control Sub-Menu	Item Specific Help
PCI Express - Root Port 1: [Auto]	
PCI Express - Root Port 2: [Auto]	
PCI Hot-Plug Resources: [Disabled]	Control the PCI Express Port via this setup option.
Root Port ASPM Support: [Auto]	Disabled - Port always disabled.
ASPM Latency Checking: [Enabled]	Auto - Only enable if card found.
	Note that if Root Port 1 is disabled, Root Ports 2-4 will be disabled as well.

F1 Help **↑↓** Select Item **-/+** Change Values F9 Setup Defaults
 Esc Exit **↔** Select Menu Enter Select **▶** Sub-Menu F10 Save and Exit

8.5.10 Intel Poulsbo USB Control

Phoenix SecureCore(tm) Setup Utility	
Intel	
Poulsbo USB Control Sub-Menu	Item Specific Help
USB Client- Device 26, Function 0: [Disabled]	Control USB Client functionality through this Setup Item.
USB - Device 29, All Functions: [Enabled]	
USB - Device 29, F2 Only: [Enabled]	

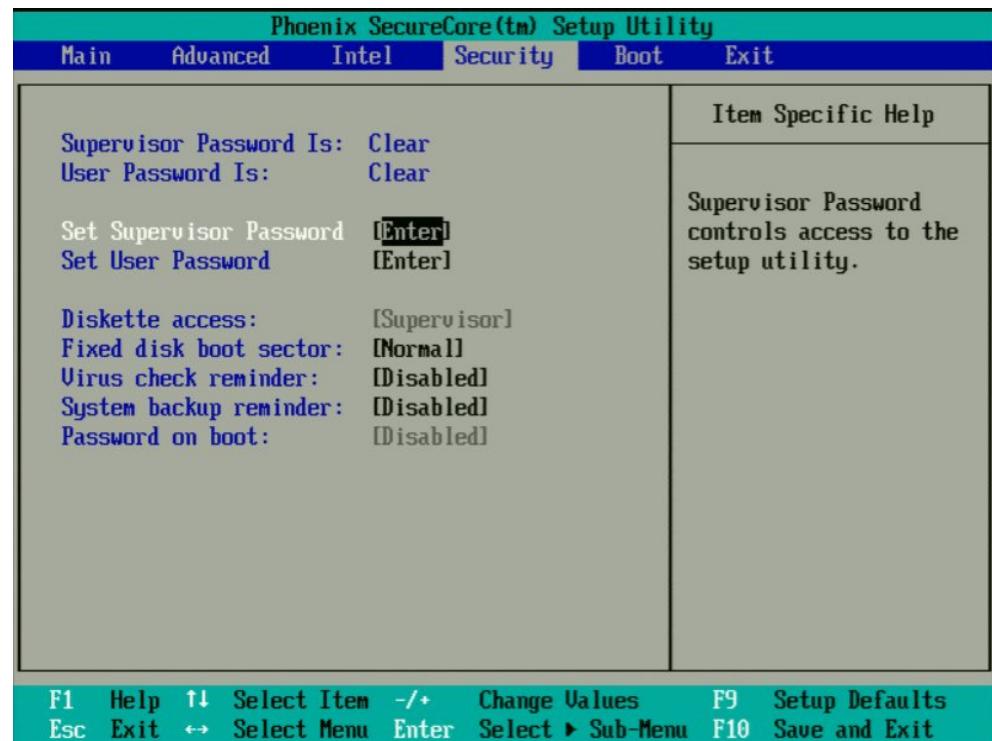
F1 Help $\uparrow\downarrow$ Select Item $-/+$ Change Values F9 Setup Defaults
 Esc Exit \leftrightarrow Select Menu Enter Select \blacktriangleright Sub-Menu F10 Save and Exit

8.5.11 Intel Video Control

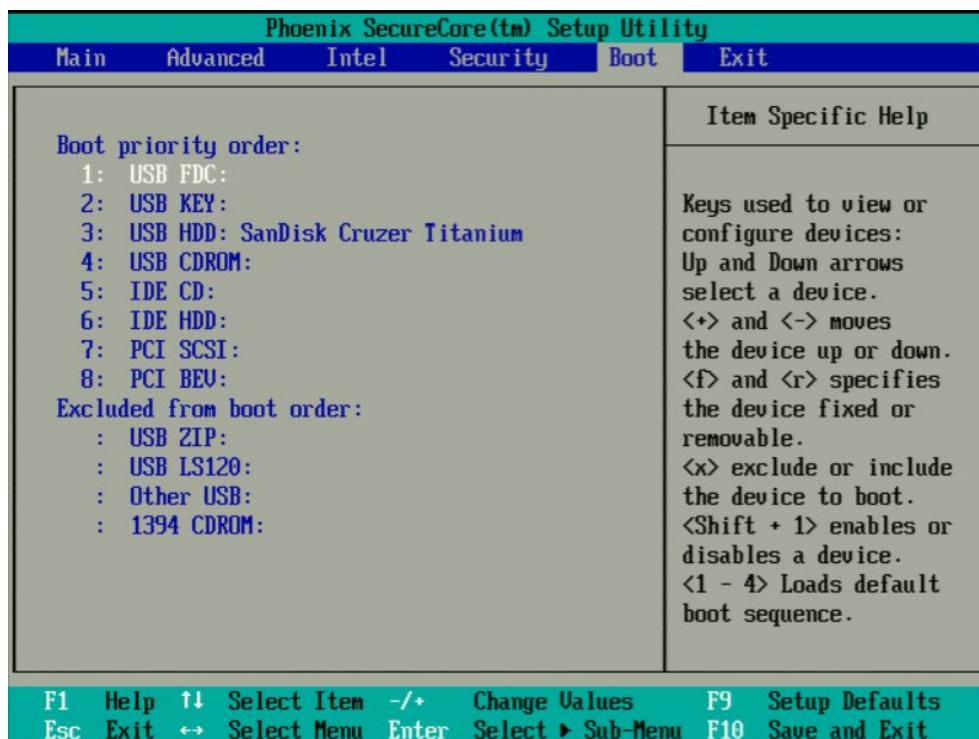
Phoenix SecureCore(tm) Setup Utility	
Intel	
Video (Intel IGD) Control Sub-Menu	Item Specific Help
IGD - Device 2: [Auto]	Enable or Disable the Internal Graphics Device by setting item to the desired value.
IGD - Boot Type: [UBIOS Default]	
IGD - S3 Popup: [Disabled]	
► IGD - LCD Control Sub-Menu	
► IGD - TV Control Sub-Menu	
Pre-Allocated Memory Size: [8MB]	
Graphic Memory Aperture Size: [256MB]	

F1 Help $\uparrow\downarrow$ Select Item $-/+$ Change Values F9 Setup Defaults
 Esc Exit \leftrightarrow Select Menu Enter Select \blacktriangleright Sub-Menu F10 Save and Exit

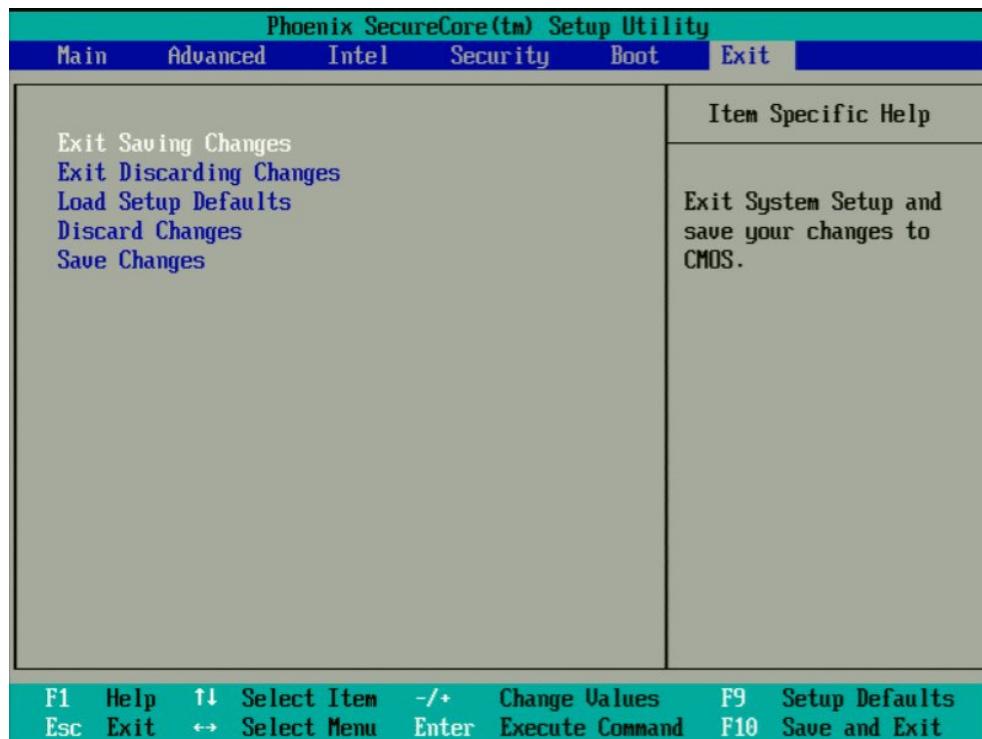
8.5.12 Security



8.5.13 Boot



8.5.14 Exit



8.6 CMOS RAM Map

Systems based on the industry-standard specification include a battery backed real-time clock (RTC) chip. This clock contains at least 64 Bytes of non-volatile RAM. The system BIOS uses this area to store information including system configuration and initialization parameters, system diagnostics, and the time and date. This information remains intact even when the system is powered down.

The BIOS supports 128 Bytes of CMOS RAM. This information is accessible through I/O ports 70h and 71h. CMOS RAM can be divided into several segments:

- » Locations 00h-0Fh contain the RTC and status information
- » Locations 10h-2Fh contain system configuration data
- » Locations 30h-3Fh contain system BIOS-specific configuration data as well as chipset-specific information
- » Locations 40h-7Fh contain chipset-specific information as well as power management configuration parameters

The following table provides a summary of how these areas may be further divided.

Beginning	Ending	Checksum	Description
00h	0Fh	No	RTC and Checksum
10h	2Dh	Yes	System Configuration
2Eh	2Fh	No	Checksum Value of 10h-2Dh
30h	33h	No	Standard CMOS
34h	3Fh	No	Standard CMOS - SystemSoft Reserved
40h	5Bh	Yes	Extended CMOS - Chipset Specific
5Ch	5Dh	No	Checksum Value of 40h-5Bh
5Eh	6Eh	No	Extended CMOS - Chipset Specific
6Fh	7Dh	Yes	Extended CMOS - Power Management
7Eh	7Fh	No	Checksum Value of 6Fh-7Dh

CMOS Map	
Location	Description
00h	Time of day (seconds) specified in BCD
01h	Alarm (seconds) specified in BCD
02h	Time of day (minutes) specified in BCD
03h	Alarm (minutes) specified in BCD
04h	Time of day (hours) specified in BCD
05h	Alarm (hours) specified in BCD
06h	Day of week specified in BCD
07h	Day of month specified in BCD
08h	Month specified in BCD
09h	Year specified in BCD
0Ah	Status Register A Bit 7 = Update in progress Bits 6-4 = Time based frequency divider Bits 3-0 = Rate selection bits that define the periodic interrupt rate and output frequency.

CMOS Map		
Location	Description	
0Bh	Status Register B	Status Register B
		Bit 7 = Run/Halt
		0 Run
		1 Halt
		Bit 6 = Periodic Timer
		0 Disable
		1 Enable
		Bit 5 = Alarm Interrupt
		0 Disable
		1 Enable
	Bit 4 = Update Ended Interrupt	Bit 4 = Update Ended Interrupt
		0 Disable
		1 Enable
	Bit 3 = Square Wave Interrupt	Bit 3 = Square Wave Interrupt
		0 Disable
		1 Enable
	Bit 2 = Calendar Format	Bit 2 = Calendar Format
		0 BCD
	Bit 1 = Time Format	1 Binary
		0 12-Hour
		1 24-Hour
	Bit 0 = Daylight Savings Time	Bit 0 = Daylight Savings Time
		0 Disable
		1 Enable
0Ch	Status Register C	
	Bit 7 =	Interrupt Flag
	Bit 6 =	Periodic Interrupt Flag
	Bit 5 =	Alarm Interrupt Flag
	Bit 4 =	Update Interrupt Flag
	Bits 3-0 =	Reserved
0Dh	Status Register D	
	Bit 7 =	Realtime Clock
	0	Lost Power
	1	Power
0Eh	CMOS Location for Bad CMOS and Checksum Flags	
	Bit 7 =	Flag for CMOS Lost Power
	0 =	Power OK
	1 =	Lost Power
	Bit 6 =	Flag for CMOS checksum bad
	0 =	Checksum is valid
	1 =	Checksum is bad
0Fh	Shutdown Code	
10h	Diskette Drives	
	Bits 7-4 =	Diskette Drive A
	0000 =	Not installed
	0001 =	Drive A = 360 kB
	0010 =	Drive A = 1.2MB
	0011 =	Drive A = 720 kB
	0100 =	Drive A = 1.44MB
	0101 =	Drive A = 2.88MB
	Bits 3-0 =	Diskette Drive B
	0000 =	Not installed
	0001 =	Drive B = 360 kB
	0010 =	Drive B = 1.2MB
	0011 =	Drive B = 720 kB
	0100 =	Drive B = 1.44MB
	0101 =	Drive B = 2.88MB
11h	Reserved	

CMOS Map	
Location	Description
12h	<p>Fixed (Hard) Drives</p> <p>Bits 7-4 = Hard Drive 0, AT Type 0000 = Not installed 0001-1110 = Types 1-14 1111 = Extended drive types 16-44. See location 19h.</p> <p>Bits 3-0 = Hard Drive 1, AT Type 0000 = Not installed 0001-1110 = Types 1-14 1111 = Extended drive types 16-44. See location 2Ah.</p>
13h	Reserved
14h	<p>Equipment</p> <p>Bits 7-6 = Number of Diskette Drives 00 = One diskette drive 01 = Two diskette drives 10, 11 = Reserved</p> <p>Bits 5-4 = Primary Display Type 00 = Adapter with option ROM 01 = CGA in 40 column mode 10 = CGA in 80 column mode 11 = Monochrome</p> <p>Bits 3-2 = Reserved</p> <p>Bit 1 = Math Coprocessor Presence 0 = Not installed 1 = Installed</p> <p>Bit 0 = Bootable Diskette Drive 0 = Not installed 1 = Installed</p>
15h	Base Memory Size (in kB) - Low Byte
16h	Base Memory Size (in kB) - High Byte
17h	Extended Memory Size (in kB) - Low Byte
18h	Extended Memory Size (in kB) - High Byte
19h	Extended Drive Type - Hard Drive 0
1Ah	Extended Drive Type - Hard Drive 1
1Bh	<p>Custom and Fixed (Hard) Drive Flags</p> <p>Bits 7-6 = Reserved</p> <p>Bit 5 = Internal Floppy Disk Controller 0 = Disabled 1 = Enabled</p> <p>Bit 4 = Internal IDE Controller 0 = Disabled 1 = Enabled</p> <p>Bit 3 = Hard Drive 0 Custom Flag 0 = Disabled 1 = Enabled</p> <p>Bit 2 = Hard Drive 0 IDE Flag 0 = Disabled 1 = Enabled</p> <p>Bit 1 = Hard Drive 1 Custom Flag 0 = Disabled 1 = Enabled</p> <p>Bit 0 = Hard Drive 1 IDE Flag 0 = Disabled 1 = Enabled</p>
1Ch	Reserved
1Dh	EMS Memory Size Low Byte
1Eh	EMS Memory Size High Byte
1Fh - 24h	<p>Custom Drive Table 0</p> <p>These 6 Bytes (48 bits) contain the following data:</p> <p>Cylinders 10bits range 0-1023 Landing Zone 10bits range 0-1023 Write Precompensation 10bits range 0-1023 Heads 8bits range 0-15 Sectors/Track 8bits range 0-254</p>

CMOS Map	
Location	Description
1Fh	Byte 0 Bits 7-0 = Lower 8 bits of Cylinders
20h	Byte 1 Bits 7-2 = Lower 6 bits of Landing Zone Bits 1-0 = Upper 2 bits of Cylinders
21h	Byte 2 Bits 7-4 = Lower 4 bits of Write Precompensation Bits 3-0 = Upper 4 bits of Landing Zone
22h	Byte 3 Bits 7-6 = Reserved Bits 5-0 = Upper 6 bits of Write Precompensation
23h	Byte 4 Bits 7-0 = Number of Heads
24h	Byte 5 Bits 7-0 = Sectors Per Track
25h - 2Ah	Custom Drive Table 1 These 6 Bytes (48 bits) contain the following data: Cylinders 10bits range 0-1023 Landing Zone 10bits range 0-1023 Write Precompensation 10bits range 0-1023 Heads 8bits range 0-15 Sectors/Track 8bits range 0-254
25h	Byte 0 Bits 7-0 = Lower 8 bits of Cylinders
26h	Byte 1 Bits 7-2 = Lower 6 bits of Landing Zone Bits 1-0 = Upper 2 bits of Cylinders
27h	Byte 2 Bits 7-4 = Lower 4 bits of Write Precompensation Bits 3-0 = Upper 4 bits of Landing Zone
28h	Byte 3 Bits 7-6 = Reserved Bits 5-0 = Upper 6 bits of Write Precompensation
29h	Byte 4 Bits 7-0 = Number of Heads
2Ah	Byte 5 Bits 7-0 = Sectors Per Track
2Bh	Boot Password Bit 7 = Enable/Disable Password 0 = Disable Password 1 = Enable Password Bits 6-0 = Calculated Password
2Ch	SCU Password Bit 7 = Enable/Disable Password 0 = Disable Password 1 = Enable Password Bits 6-0 = Calculated Password
2Dh	Reserved
2Eh	High Byte of Checksum - Locations 10h to 2Dh
2Fh	Low Byte of Checksum - Locations 10h to 2Dh
30h	Extended RAM (kB) detected by POST - Low Byte
31h	Extended RAM (kB) detected by POST - High Byte
32h	BCD Value for Century
33h	Base Memory Installed Bit 7 = Flag for Memory Size 0 = 640kB 1 = 512kB Bits 6-0 = Reserved
34h	Minor CPU Revision Differentiates CPUs within a CPU type (i.e., 486SX vs 486 DX, vs 486 DX/2). This is crucial for correctly determining CPU input clock frequency. During a power-on reset, Reg DL holds minor CPU revision.
35h	Major CPU Revision Differentiates between different CPUs (i.e., 386, 486, Pentium). This is crucial for correctly determining CPU input clock frequency. During a power-on reset, Reg DH holds major CPU revision.

CMOS Map	
Location	Description
36h	<p>Hotkey Usage</p> <p>Bits 7-6 = Reserved</p> <p>Bit 5 = Semaphore for Completed POST</p> <p>Bit 4 = Semaphore for 0 Volt POST (not currently used)</p> <p>Bit 3 = Semaphore for already in SCU menu</p> <p>Bit 2 = Semaphore for already in PM menu</p> <p>Bit 1 = Semaphore for SCU menu call pending</p> <p>Bit 0 = Semaphore for PM menu call pending</p>
40h-7Fh	Definitions for these locations vary depending on the chipset.

9 Appendix A: Document Revision History

Revision	Date	Edited by	Changes
100	04.Jan.2010	WAS	Initial version from BRM 03.2009
101	19.Oct.2010	WAS	BIOS History updated. User-defined paper formatting corrected to A4 in Manual Template
102	02.Feb.2011	WAS	Preface corrected. BSP screen shot & web links changed to KCC AG.

10 Index

A

AC97 Sound 19

B

BIOS 32

BIOS History 32

BIOS Setup 37

Boot 43

C

CMOS RAM Map 45

Console Redirection 39

Copyright 4

Core BIOS Download 36

Core BIOS Functions 34

Corporate Offices 53

CPU Config 40

CPU Thermal Config 40

D

Diagnostics 29

Display Driver 17

Document Revision History 50

Documentation 4

Driver Installation 11

 AC97-Sound 14

 Chipset 12

 LAN 13

 RAID 14

 VGA 12

 W2k/XP 25

 Windows 2000 & XP 11

 Windows-NT 26

E

ELinos 10

Environmental Protection 5

Exit 44

I

I/O Config 38

Incompatibilities 8

Int15 Emulator Driver for Windows 24, 28

Int15 Hardware 24

Int15 Windows Software 25, 28

Intel Config 39

Introduction 8

K

Keystroke Controls 37

L

Linux 10

M

Microsoft Windows 9

Microsoft Windows CE 9

Microsoft Windows XPe 9

O

Operating Systems Compatibility 9

P

PCI Express Config 41

Phoenix SecureCore™ Check Point Lists 29

POST Code Checkpoints 29

Poulsbo Config 41

Power Management 21

Programming Int15dl 26

Q

QNX 10

R

Real-time OS 10

RoHS 5

S

Security 43

SFI 22

SLAX 10

Special Function Interface 22

Specification

BIOS 33

SpeedStep 20

SQS 7

Standard Features 8

Standards 4

Swiss Association for Quality and Management

Systems 7

Swiss Quality 6

T

Technical Support 5

Trademarks 4

U

USB Config 42

V

Video Config 42

VxWorks 10

W

Warranty 4

WEEE 6

Corporate Offices

Europe, Middle East & Africa

Kontron AG
Oskar-von-Miller-Strasse 1
85386 Eching/Munich
Germany
Tel.: +49 (0)8165/ 77 777
Fax: +49 (0)8165/ 77 219
info@kontron.com

Switzerland

Kontron Compact Computers AG
Nordstrasse 11/F
CH – 4542 Luterbach
Switzerland
Tel.: +41 (0)32 681 58 00
Fax: +41 (0)32 681 58 01
infokcc@kontron.com

